Public Comments on Interim Rule
"Encryption Items"
63 FR 50516, September 22, 1998

Federal Register Notice

1. William A. Root	**October 6, 1998**
2. Regulations and Procedures Technical Advisory Committee (RPTAC)	**November 2, 1998**
3. Microsoft	**November 6, 1998**
4. Investment Company Institute	**November 6, 1998**
5. VISA	**November 6, 1998**
6. Citibank	**November 6, 1998**
7. Steptoe & Johnson	**November 13, 1998**

and (a)(2) of this AD, in accordance with Heath Tecna Service Bulletin H0655-33-01, dated March 28, 1996.

(1) Perform a visual inspection to detect discrepancies (i.e., damage, burn marks, and black or brown discoloration) of the electrical plugs and receptacles of the sidewall lighting system in the passenger cabin, and to verify that the ends of all pins and sockets are even and that they are seated and locked into place, in accordance with the service bulletin. If any discrepancy is detected, prior to further flight, replace the discrepant part with a new part in accordance with the service bulletin.

(2) Modify the electrical wiring and connectors of the sidewall lighting system in the passenger cabin in accordance with paragraph 2.H. of the Accomplishment Instructions of the service bulletin.

(b) An alternative method of compliance or adjustment of the compliance time that provides an acceptable level of safety may be used if approved by the Manager, Seattle Aircraft Certification Office (ACO), FAA, Transport Airplane Directorate. Operators shall submit their requests through an appropriate FAA Principal Maintenance Inspector, who may add comments and then send it to the Manager, Seattle ACO.

Note 2: Information concerning the existence of approved alternative methods of compliance with this AD, if any, may be obtained from the Seattle ACO.

(c) Special flight permits may be issued in accordance with sections 21.197 and 21.199 of the Federal Aviation Regulations (14 CFR 21.197 and 21.199) to operate the airplane to a location where the requirements of this AD can be accomplished.

(d) The actions shall be done in accordance with Heath Tecna Service Bulletin H0655-33-01, dated March 28, 1996. This incorporation by reference was approved by the Director of the Federal Register in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. Copies may be obtained from Hexcel Interiors (formerly Heath Tecna Aerospace), 3225 Woburn Street, Bellingham, Washington 98226. Copies may be inspected at the FAA, Transport Airplane Directorate, 1601 Lind Avenue, SW., Renton, Washington; or at the Office of the Federal Register, 800 North Capitol Street, NW., suite 700, Washington, DC.

(e) This amendment becomes effective on October 27, 1998.

Issued in Renton, Washington, on September 15, 1998.

Darrell M. Pederson,

Acting Manager, Transport Airplane Directorate, Aircraft Certification Service.

[FR Doc. 98-25145 Filed 9-21-98; 8:45 am]

BILLING CODE 4910-13-U

DEPARTMENT OF COMMERCE

Bureau of Export Administration

15 CFR Parts 732, 734, 740, 742, 743, 748, 750, 752, 770, 772, and 774

[Docket No. 980911233-8233-01]

RIN 0694-AB80

Encryption Items

AGENCY: Bureau of Export Administration, Commerce.

ACTION: Interim rule.

SUMMARY: This interim rule amends the Export Administration Regulations (EAR) by clarifying controls on the export and reexport of encryption items (EI) controlled for "EI" reasons on the Commerce Control List. This rule incorporates public comments on an interim rule published in the **Federal Register** on December 30, 1996, and implements new licensing policies for general purpose non-recoverable non-voice encryption commodities or software of any key length for distribution to banks and financial institutions in specified countries.

DATES: Effective Date: This rule is effective September 22, 1998. Comments: Comments on this rule must be received on or before November 6, 1998.

ADDRESSES: Written comments on this rule should be sent to Nancy Crowe, Regulatory Policy Division, Bureau of Export Administration, Department of Commerce, P.O. Box 273, Washington, DC 20044.

FOR FURTHER INFORMATION CONTACT: James Lewis, Office of Strategic Trade and Foreign Policy Controls, Bureau of Export Administration, Telephone: (202) 482-0092.

SUPPLEMENTARY INFORMATION:

Background

On December 30, 1996, the Bureau of Export Administration (BXA) published in the **Federal Register** (61 FR 68572) an interim rule that exercises jurisdiction over, and imposes new combined national security and foreign policy controls on, certain encryption items that were on the United States Munitions List, consistent with Executive Order (E.O.) 13026 and pursuant to the Presidential Memorandum of that date, both issued by President Clinton on November 15, 1996.

BXA received comments from 45 commenters, and the comments fall into three broad categories: general concerns and objections to the policy embodied in the regulations; recommendations for specific changes or clarifications to the regulations that are consistent with the broad encryption policy implemented in the December 30 rule; and recommendations for additional changes to encryption policy.

Suggestions for Changes to Clarify Existing Policy

A number of commenters provided specific suggestions for changes or clarifications which are consistent with the intent of the policy and which would streamline or improve the regulations. Many of these suggestions are implemented in this rule, such as clarifying that the tools of trade provisions of License Exception TMP and License Exception BAG apply globally and clarifying that anti-virus software does not require a license for export.

Several commenters asked the Department of Commerce to adopt exemptions to license requirements which were available for encryption exporters under § 123.16(b)(2) and (b)(9) of the International Traffic and Arms Regulations (ITAR), such as those which allowed the export of components to a U.S. subsidiary or which allowed the export of spare parts and components without a license for an already approved sale. This rule adds these new provisions under License Exception TMP, making them applicable to encryption controlled items as well as other items eligible for TMP treatment.

Two commenters asked that the regulations clarify that the ITAR licensing policy for equipment specially made for and limited to the encryption of interbanking transactions had not changed with the transfer of jurisdiction of encryption products to the Department of Commerce. This interim rule clarifies that this equipment is not subject to EI controls.

Several commenters recommended a number of changes to the Key Escrow Product and Agent criteria found in Supplement Nos. 4 and 5 part to 742 of the EAR. These recommendations were to simplify the criteria, and to modify some of the specific prescriptions to allow for greater flexibility and variation on the part of exporters. Many commenters found the criteria too bureaucratic and legalistic to help advance U.S. encryption policy goals, while others noted that the criteria were still overly focused on key escrow and not consistent with the broader approach to key recovery found elsewhere in the regulation. Several commenters also encouraged the administration to make clear that it had moved beyond key escrow to key recovery in its policy. One commenter

focused on weaknesses and omissions found in the key escrow product and agent criteria found in Supplement Nos. 4 and 5 to part 742 of the EAR, and provided suggested additions to the criteria to make them more consistent with emerging business practices. The criteria specified in Supplement Nos. 4 and 5 were discussed extensively with industry prior to publication of the December 30 interim rule, and the rule reflects these discussions. However, BXA continues to look for ways to streamline the criteria, and will address revisions in a future regulation.

Several commenters expressed concerns over the longer processing time required for licenses at the Department of Commerce. Some commenters noted that the involvement of Departments of Energy and State, the Arms Control and Disarmament Agency and other agencies which did not review license applications for encryption products submitted to the Department of State added unnecessary levels of review and caused unwarranted delays. BXA is continuing to work with other reviewing Departments and Agencies to ensure expeditious review of encryption license applications. Many commenters noted that the requirements for a Department of Commerce license were substantially greater than what was required at the Department of State. The Department of Commerce, for example, requires an end-use certificate to be obtained for some destinations before approving an export; the Department of State did not and exporters question the need for this change. Other commenters noted that the Department of State licensing system was more flexible and faster for approvals of distribution and manufacturing arrangements. The Department of Commerce has no equivalent licenses, but is reviewing the possibility of such licenses. Many oral comments received since the close of the comment period note that unlike the Department of State, the Department of Commerce does not allow licenses to be amended, so that if an exporter has, for example, a license which allows him to ship to thirty countries and wishes to add one more, the Department of Commerce requires submission of an entire new license while the Department of State was content with a simple letter noting the requested change. This rule will now allow the addition of countries to an Encryption Licensing Arrangement by letter. BXA understands industry concerns about the license process under the EAR, and continues to look for ways to streamline the process.

Additional Recommendations for Changes to Encryption Policy

A number of commenters asked that the Administration revisit a number of decisions made in the course of the development of the encryption policy as reflected in the December 30 interim rule. Several asked that we reconsider and liberalize the treatment of Cryptographic Application Program Interface. Others questioned the addition of "defense services" controls similar to that contained in the ITAR (which prohibits U.S. persons from assisting foreign entities from developing their own indigenous encryption products). Several commenters objected to the structure of License Exception KMI for non-recoverable 56 bit products, with its requirement for a review every six months. Other commenters also called for a reversal of the decision to exempt transferred encryption items from normal Department of Commerce regulatory practices. Finally, several commenters recommended that the licensing criteria and License Exceptions applicable to other dual-use items be fully applicable to encryption products, such as considerations of foreign availability, the *de minimis* content exclusion, public domain treatment and the use of License Exceptions. This rule focuses on clarifications to existing encryption policy.

Based on public comments to the December 30 interim rule, this interim rule specifically makes the following changes:

—In §§ 732.2(d) and 732.3(e)(2), makes editorial corrections to clarify that encryption items controlled for "EI" reasons under ECCNs 5A002, 5D002 and 5E002 are not eligible for *De Minimis* treatment.

—In § 734.2, clarifies that downloading or causing the downloading of encryption source code and object code in Canada is not controlled and does not require a license.

—In § 740.6, clarifies that letters of assurance required for exports under License Exception TSR may be accepted in the form of a letter or any other written communication from the importer, including communications via facsimile.

—§ 740.8 is also amended by adding a new paragraph to authorize, after a one-time technical review, exports and reexports under License Exception KMI of non-recoverable financial-specific encryption software (which is not eligible under the provisions of License Exception TSU for mass market software, such as SET or similar protocols) and commodities of any key length that are restricted by design (e.g., highly field-formatted with validation procedures, and not easily diverted to other end-uses) for financial applications to secure financial transactions, for end-uses such as financial transfers or electronic commerce. No business and marketing plan to develop, produce, or market encryption items with recoverable features is required. Such exports and reexports are eligible to all destinations except Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria. Conforming changes are also made in § 742.15.

—§ 740.8 is also amended to authorize, after a one time review, exports and reexports under License Exception KMI of general purpose non-recoverable non-voice encryption commodities or software of any key length for distribution to banks and financial institutions (as defined in part 772 of the EAR) in destinations listed in new Supplement No. 3 to part 740, provided the end-use is limited to secure business financial communications or transactions or financial communications/ transactions between the bank or financial institution and its customers. No customer to customer communications or transactions are permitted. Software and commodities that have already received a one-time technical review through a classification request or have been licensed for export under an Encryption Licensing Arrangement or a license are eligible for export to banks and financial institutions under License Exception KMI without an additional one-time technical review. Note that no business or marketing plan is required. Conforming changes are also made in § 742.15. Software and commodities that have already been approved under an Encryption Licensing Arrangement to banks in specified countries may now be exported or reexported to other banks and financial institutions in those countries under the same Encryption Licensing Arrangement.

—In § 740.9, removes the reference to Country Group D:1. With this change, commodities and software are eligible for export under the tools of trade provisions of License Exception TMP to all destinations except countries listed in country group E:2 or Sudan. This also clarifies that encryption software controlled for EI reasons under ECCN 5D002 may be pre-loaded on a laptop and temporarily exported under the tools of trade provisions of License Exception TMP

to most countries, including those listed in Country Group D:1.

—Also in § 740.9, adds a new paragraph (a)(2)(ix) to authorize under License Exception TMP the export of components, parts, tools or test equipment exported by a U.S. person to its subsidiary, affiliate or facility in a country in Country Group B that is owned or controlled by the U.S. person, if the components, part, tool or test equipment is to be used for manufacture, assembly, testing, production or modification, provided that no components, parts, tools or test equipment or the direct product of such components, parts, tools or test equipment are transferred or reexported to a country other than the United States from such subsidiary, affiliate or facility without a license or other authorization from BXA.

—In § 740.11, excludes items controlled for EI reasons from eligibility under the International Safeguards provisions of License Exception GOV.

—In § 740.14, clarifies existing provisions of License Exception BAG to distinguish temporary from permanent exports and imposes a restriction on the use of BAG for exports or reexports of EI-controlled items to terrorist supporting destinations or by persons other than U.S. citizens and permanent residents.

—New Supplement No. 3 to part 740 is added to list the countries eligible to receive under License Exception KMI general purpose non-recoverable non-voice encryption commodities or software of any key length for distribution to banks and financial institutions.

—In § 742.15, adds 40-bit DES as being eligible for consideration under the 15-day review, for mass-market eligibility, subject to the additional criteria listed in Supplement No. 6 to part 742.

—In § 742.15(b)(1), clarifies that subsequent bundling, updates or releases may be exported and reexported under applicable provisions of the EAR without a separate one-time technical review so long as the functional encryption capacity of the originally reviewed mass-market encryption software has not been modified or enhanced.

—New paragraph (b)(4) is added to § 742.15 to authorize exports and reexports under an Encryption Licensing Arrangement of general purpose non recoverable, non-voice encryption commodities and software of any key length for use by banks/financial institutions as defined in part 772 of the EAR in all destinations except Cuba, Iran, Iraq, Libya, North Korea, Syria and Sudan. No business or marketing plan is required. Exports and reexports for the end-uses to secure business financial communications or between the bank and/or financial institution and its customers will receive favorable consideration. No customer to customer communications or transactions are eligible under the Encryption Licensing Arrangement.

—In Supplement No. 4 to part 742, paragraph (3), revises "reasonable frequency" to "at least once every three hours" to resolve the ambiguity on how often the output must identify the key recovery agent and material/information required to decrypt the ciphertext.

—In Supplement No. 4 to part 742, paragraph (6)(i), clarifies that the U.S. government must be able to obtain the key(s) or other material/information needed to decrypt all data, without restricting the means by which the key recoverable products allow this.

—In Supplement No. 6 to part 742 for 7-day mass-market classification requests, clarifies that a copy of the encryption subsystem source code may be used instead of a test vector to determine eligibility for License Exception TSU for mass market software.

—In § 743.1, requires reporting under the Wassenaar Arrangement for items controlled under ECCNs 5A002 and 5D002 when exported under specific provisions of License Exception KMI. This is not a new reporting requirement, but replaces and narrows the scope of the reporting requirement under the Encryption License Arrangement for financial-specific commodities and software and general purpose non-recoverable non-voice encryption commodities and software of any key length for distribution to banks and financial institutions that are eligible for License Exception KMI.

—In §§ 748.9 and 748.10, clarifies a long-standing policy that no support documentation is required for exports of technology or software, and it removes the requirement for such support documentation for exports of technology or software to Bulgaria, Czech Republic, Hungary, Poland, Romania, or Slovakia. This rule also exempts from support documentation requirements all encryption items controlled under ECCNs 5A002, 5B002, 5D002 and 5E002. This conforms with the practice under the ITAR prior to December 30, 1996.

—In § 750.7, allows requests to add countries of destination to Encryption Licensing Arrangements by letter.

—In § 752.3, excludes encryption items controlled for EI reasons from eligibility for a Special Comprehensive License.

—In § 770.2, adds a new interpretation to clarify that encryption software controlled for EI reasons under ECCN 5D002 may be pre-loaded on a laptop and exported under the tools of trade provision of License Exception TMP or the personal use exemption under License Exception BAG, subject to the terms and conditions of such License Exceptions.

—In part 772, adds new definitions for "bank", "effective control", "encryption licensing arrangement", and "financial institution".

—In Supplement No. 1 to part 774, Category 5—Telecommunications and Information Security is amended by revising ECCN 5A002 to authorize exports of components and spare parts under License Exception LVS, provided the value of each order does not exceed $500 and the components and spare parts are destined for items previously authorized for export, and to clarify that equipment for the encryption of interbanking transactions is not controlled under that entry.

—Revises the phrase "up to 56-bit key length DES" where it appears to read "56-bit DES or equivalent", and makes other editorial changes.

Note that this rule does not affect exports or reexports authorized under licenses issued prior to the effective date of this rule.

Several commenters also noted that the exemptions found under § 125.4(b) of the ITAR should be implemented in the EAR. Most of the exemptions found in § 125.4(b) of the ITAR are already available under existing provisions of the EAR. For example, § 125.4(b)(4) of the ITAR authorizes exports without a license of copies of technical data previously authorized for export. The EAR has no restrictions on the number of copies sent to a consignee authorized to receive technology under license or a License Exception. Section 125.4(b)(5) authorizes exports without a license of technical data in the form of basic operations, maintenance, and training information relating to a defense article lawfully exported or authorized for export provided the technical data is for use by the same recipient. Further, Section 125.4(2) authorizes exports of technical data in furtherance of a manufacturing license or technical assistance agreement. License Exception

TSU for operation technology and software (see § 740.13 of the EAR) authorizes the export and reexport of the minimum technology necessary for the installation, operation, maintenance and repair of those products (including software) that are lawfully exported or reexported under a license, a License Exception, or non license required (NLR). Section 125.4(b)(7) of the ITAR allows the return of technical data to the original source of import. License Exception TMP similarly authorizes the return of any foreign-origin item, including technology, to the country from which it was imported if the characteristics have not been enhanced while in the United States (see § 740.9(b)(3) of the EAR).

BXA has also received many inquiries on Shipper's Export Declaration (SED) requirements for Canada. Note that the EAR do not require exporters to file an SED for exports of any item to Canada for consumption in Canada, unless a license is required. Further note that a license is not required for exports of encryption items for consumption in Canada, including certain exports over the Internet. Finally, BXA has received many requests for clarification on SED requirements for electronic transfers. Neither the EAR nor the FTSR provide for the filing of SEDs for electronic transfers of items controlled by the Department of Commerce under the EAR .

As further clarifications and changes to the encryption provisions of the EAR are intended, in particular regarding Supplement Nos. 4 and 5 to part 742 of the EAR, BXA will publish additional interim rules in the **Federal Register**.

Rulemaking Requirements

1. This interim rule has been determined to be significant for purposes of E. O. 12866.

2. Notwithstanding any other provision of law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with a collection of information, subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid Office of Management and Budget Control Number. This rule contains collections of information subject to the Paperwork Reduction Act of 1980 (44 U.S.C. 3501 *et seq.*). These collections have been approved by the Office of Management and Budget under control numbers 0694–0088, "Multi-Purpose Application," which carries a burden hour estimate of 52.5 minutes per submission; and 0694–0104, "Commercial Encryption Items Transferred from the Department of State to the Department of Commerce," which carries the following burden hours: marketing plans (40 hours each); semiannual progress reports (8 hours each); safeguard procedures (4 hours); recordkeeping (2 hours); annual reports (4 hours); and Encryption Licensing Arrangement letters (15 minutes).

3. This rule does not contain policies with Federalism implications sufficient to warrant preparation of a Federalism assessment under E.O. 12612.

4. The provisions of the Administrative Procedure Act (5 U.S.C. 553) requiring notice of proposed rulemaking, the opportunity for public participation, and a delay in effective date, are inapplicable because this regulation involves a military and foreign affairs function of the United States (Sec. 5 U.S.C. 553(a)(1)). Further, no other law requires that a notice of proposed rulemaking and an opportunity for public comment be given for this interim final rule. Because a notice of proposed rulemaking and an opportunity for public comment are not required to be given for this rule under 5 U.S.C. or by any other law, the requirements of the Regulatory Flexibility Act (5 U.S.C. 601 *et seq.*) are not applicable.

However, because of the importance of the issues raised by these regulations, this rule is issued in interim form and comments will be considered in the development of final regulations. Accordingly, the Department of Commerce encourages interested persons who wish to comment to do so at the earliest possible time to permit the fullest consideration of their views.

The period for submission of comments will close November 6, 1998. The Department of Commerce will consider all comments received before the close of the comment period in developing final regulations. Comments received after the end of the comment period will be considered if possible, but their consideration cannot be assured. The Department will not accept public comments accompanied by a request that a part or all of the material be treated confidentially because of its business proprietary nature or for any other reason. The Department of Commerce will return such comments and materials to the person submitting the comments and will not consider them in the development of final regulations. All public comments on these regulations will be a matter of public record and will be available for public inspection and copying. In the interest of accuracy and completeness, the Department of Commerce requires comments in written form.

Oral comments must be followed by written memoranda, which will also be a matter of public record and will be available for public review and copying. Communications from agencies of the United States Government or foreign governments will not be made available for public inspection.

The public record concerning these regulations will be maintained in the Bureau of Export Administration Freedom of Information Records Inspection Facility, Room 4525, Department of Commerce, 14th Street and Pennsylvania Avenue, NW, Washington, DC 20230. Records in this facility, including written public comments and memoranda summarizing the substance of oral communications, may be inspected and copied in accordance with regulations published in Part 4 of Title 15 of the Code of Federal Regulations (CFR). Information about the inspection and copying of records at the facility may be obtained from Margaret Cornejo, Bureau of Export Administration Freedom of Information Officer, at the above address or by calling (202) 482–5653.

List of Subjects

15 CFR Parts 732, 740, 743, 748, 750, and 752

Administrative practice and procedure, Exports, Foreign trade, Reporting and recordkeeping requirements.

15 CFR Part 734

Administrative practice and procedure, Exports, Foreign trade.

15 CFR Parts 742, 770, 772 and 774

Exports, foreign trade.

Accordingly, 15 CFR chapter VII, subchapter C, is amended as follows:

1. The authority citation for 15 CFR parts 732, 740, 748, 752 and 772 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; Executive Order 13026 (November 15, 1996, 61 FR 58767); Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

2. The authority citation for 15 CFR part 734 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; Executive Order 13026 (November 15, 1996, 61 FR 58767); Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

3. The authority citation for 15 CFR part 742 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; 18 U.S.C. 2510 *et seq.*;

22 U.S.C. 3201 *et seq.*; 42 U.S.C. 2139a; E.O. 12058, 43 FR 20947, 3 CFR, 1978 Comp., p. 179; E.O. 12851, 58 FR 33181, 3 CFR, 1993 Comp., p. 608; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; Executive Order 13026 (November 15, 1996, 61 FR 58767); Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

4. The authority citation for 15 CFR part 743 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

5. The authority citation for 15 CFR part 750 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; Notice of August 15, 1995 (60 FR 42767, August 17, 1995); E.O. 12981, 60 FR 62981; Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

6. The authority citation for 15 CFR part 770 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

7. The authority citation for 15 CFR part 774 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; 10 U.S.C. 7420; 10 U.S.C. 7430(e); 18 U.S.C. 2510 *et seq.*; 22 U.S.C. 287c; 22 U.S.C. 3201 *et seq.*; 22 U.S.C. 6004; Sec. 201, Pub. L. 104–58, 109 Stat. 557 (30 U.S.C. 185(s)); 30 U.S.C. 185(u); 42 U.S.C. 2139a; 42 U.S.C. 6212; 43 U.S.C. 1354; 46 U.S.C. app. 466c; 50 U.S.C. app. 5; E.O. 12924, 59 FR 43437, 3 CFR, 1994 Comp., p. 917; Executive Order 13026 (November 15, 1996, 61 FR 58767); Notice of August 17, 1998 (63 FR 55121, August 17, 1998).

PART 732—[AMENDED]

§ 732.2 [Amended]

8. Section 732.2(d) amended by revising the phrase "ECCN 5A002 or ECCN 5D002" to read "ECCNs 5A002, 5D002 or 5E002".

§ 732.3 [Amended]

9. Section 732.3(e)(2) is amended by revising the phrase "ECCN 5A002 or ECCN 5D002" to read "ECCNs 5A002, 5D002 or 5E002".

PART 734—[AMENDED]

10. Section 734.2 is amended by revising paragraph (b)(9)(ii) to read as follows:

§ 734.2 Important EAR terms and principles.

(a) * * *
(b) * * *
(9) * * *

(ii) The export of encryption source code and object code software controlled for EI reasons under ECCN 5D002 on the Commerce Control List (see Supplement No. 1 to part 774 of the EAR) includes downloading, or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S. (except Canada), or making such software available for transfer outside the United States (except Canada), over wire, cable, radio, electromagnetic, photo optical, photoelectric or other comparable communications facilities accessible to persons outside the United States (except Canada), including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites, unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code outside the United States or Canada. Such precautions shall include ensuring that the facility from which the software is available controls the access to and transfers of such software through such measures as:

(A) The access control system, either through automated means or human intervention, checks the address of every system requesting or receiving a transfer and verifies that such systems are located within the United States or Canada;

(B) The access control system provides every requesting or receiving party with notice that the transfer includes or would include cryptographic software subject to export controls under the Export Administration Regulations, and that anyone receiving such a transfer cannot export the software without a license; and

(C) Every party requesting or receiving a transfer of such software must acknowledge affirmatively that he or she understands that the cryptographic software is subject to export controls under the Export Administration Regulations and that anyone receiving the transfer cannot export the software without a license. BXA will consider acknowledgments in electronic form provided that they are adequate to assure legal undertakings similar to written acknowledgments.

* * * * *

§ 734.4 [Amended]

11. Section 734.4 is amended by revising the phrase "ECCN, 5A002, ECCN 5D002, and 5E002" in paragraph (b)(2) to read "ECCNs 5A002, 5D002, and 5E002".

PART 740—[AMENDED]

12. Section 740.3 is amended by adding a new paragraph (d)(5) to read as follows:

§ 740.3 Shipments of limited value (LVS).

* * * * *

(d) * * *

(5) *Exports of encryption items.* For components or spare parts controlled for "EI" reasons under ECCN 5A002, exports under this License Exception must be destined to support an item previously authorized for export.

* * * * *

13. Section 740.6 is amended by revising the first sentence in paragraph (a)(3) to read as follows:

§ 740.6 Technology and software under restriction (TSR).

(a) * * *

(3) *Form of written assurance.* The required assurance may be made in the form of a letter or any other written communication from the importer, including communications via facsimile, or the assurance may be incorporated into a licensing agreement that specifically includes the assurances. * * *

* * * * *

14. Section 740.8 is amended:

(a) By revising paragraph (b)(2);

(b) By revising the phrase "recovery encryption software and equipment" in paragraph (d)(1) to read "recoverable encryption items";

(c) By revising the phrase "March 1 and no later than September 1" in paragraph (e)(2) to read "February 1 and no later than August 1", as follows:

§ 740.8 Key management infrastructure.

* * * * *

(b) * * *

(2)(i) *Non-recoverable encryption commodities and software.* Eligible items are non-recoverable 56-bit DES or equivalent strength commodities and software controlled under ECCNs 5A002 and 5D002 that are made eligible as a result of a one-time BXA review. You may initiate this review by submitting a classification request for your product in accordance with paragraph (d)(2) of this section.

(ii) *Non-recoverable financial-specific encryption commodities and software of any key length.* (A)(1) After a one-time technical review through a classification request (see § 748.3 of the EAR), non-recoverable, financial-specific encryption software (which is not eligible under the provisions of License Exception TSU for mass market software such as SET or similar protocols); and commodities of any key length that are

restricted by design (e.g., highly field-formatted with validation procedures, and not easily diverted to other end-uses) for financial applications to secure financial communications/transactions for end-uses such as financial transfers, or electronic commerce will be permitted under License Exception KMI for export and reexport to all destinations except Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.

(*2*) For such classification requests, indicate "License Exception KMI" in block #9 on Form BXA748P. Submit the original request to BXA in accordance with § 748.3 of the EAR and send a copy of the request to: Attn: Financial Specific Encryption Request Coordinator, P.O. Box 246, Annapolis Junction, MD 20701–0246.

(B) Upon approval of your classification request for a non-recoverable financial-specific encryption commodities or software, you will become eligible to use License Exception KMI. This approval allows the export or reexport of encryption commodities and software specifically designed and limited for use in the processing of electronic financial (commerce) transactions, which implements cryptography in specifically delineated fields such as merchant's identification, the customer's identification and address, the merchandise purchased, and the payment mechanism. It does not allow for encryption of data, text or other media except as directly related to these elements of the electronic transaction to support financial communications/ transactions. For exports and reexports under the provisions of this paragraph (b)(2)(ii), no business and marketing plan is required, and the reporting requirements of paragraph (e) of this section and the criteria described in Supplement Nos. 4 and 5 to part 742 of the EAR are not applicable. However, you are subject to the reporting requirements of the Wassenaar Arrangement (see § 743.1 of the EAR)

(iii) *General purpose non-recoverable encryption commodities or software of any key length for use by banks/ financial institutions.* (A)(1) After a one-time technical review through a classification request (see § 748.3 of the EAR), exports and reexports of general purpose non-recoverable non-voice encryption commodities or software of any key length will be permitted under License Exception KMI for distribution to banks and financial institutions as defined in part 772 of the EAR in all destinations listed in Supplement No. 3 to part 740 of the EAR, and to branches of such banks and financial institutions wherever located. The end-use is limited to secure business financial communications or transactions and financial communications/ transactions between the bank and/or financial institution and its customers. No customer to customer communications/ transactions are permitted.

(*2*) For such classificiation requests, indicate "License Exception KMI" in block #9 on Form BXA748P. Submit the original request to BXA in accordance with § 748.3 of the EAR and send a copy of the request to: Attn: Financial Specific Encryption Request Coordinator, P.O. Box 246, Annapolis Junction, MD 20701–0246.

(*3*) Upon approval of your classification request for a non-recoverable financial-specific encryption commodities or software, you will become eligible to use License Exception KMI.

(B) Software and commodities that have already received a one-time technical review through a classification request or have been licensed for export under an Encryption Licensing Arrangement or a license are eligible for export under the provisions of this paragraph (b)(2)(iii) without an additional one-time technical review.

(C) Software and commodities that have already been approved under an Encryption Licensing Arrangement to banks and financial institutions in specified countries may now be exported or reexported to other banks and financial institutions in those countries under the same Encryption Licensing Arrangement.

(D) For exports and reexports under the provisions of this paragraph (b)(2)(iii), no business and marketing plan is required and the reporting requirements of paragraph (e) of this section are not applicable. However, you are subject to the reporting requirements of the Wassenaar Arrangement (see § 743.1 of the EAR).

* * * * *

15. Section 740.9 is amended:

a. By revising paragraph (a)(2)(i);

b. By revising the reference to "§ 740.9(a)" in paragraph (a)(2)(ii)(C) to read "§ 740.10(a)";

c. By revising the reference to "under § 740.8(b)(1)" in the introductory text of paragraph (b)(1)(iii) to read "under this paragraph (b)(1)"; and

d. By adding a new paragraph (a)(2)(ix) to read as follows:

§ 740.9 Temporary imports, exports, and reexports (TMP).

* * * * *

(a) * * *

(2) * * *

(i) *Tools of trade.* Usual and reasonable kinds and quantities of tools of trade (commodities and software) for use by the exporter or employees of the exporter in a lawful enterprise or undertaking of the exporter. Eligible tools of trade may include, but are not limited to, such equipment and software as is necessary to commission or service goods, provided that the equipment or software is appropriate for this purpose and that all goods to be commissioned or serviced are of foreign origin, or if subject to the EAR, have been legally exported or reexported. The tools of trade must remain under the effective control of the exporter or the exporter's employee (see part 772 of the EAR for a definition of "effective control"). The shipment of tools of trade may accompany the individual departing from the United States or may be shipped unaccompanied within one month before the individual's departure from the United States, or at any time after departure. No tools of the trade may be taken to Country Group E:2 (see Supplement No. 1 to part 740) or Sudan. For exports under this License Exception of laptop computers loaded with encryption software, refer to item interpretation 13 in § 770.2 of the EAR.

* * * * *

(ix) *Temporary exports to a U.S. subsidiary, affiliate or facility in Country Group B.* (A) Components, parts, tools or test equipment exported by a U.S. person to its subsidiary, affiliate or facility in a country listed in Country Group B (see Supplement No. 1 to this part) that is owned or controlled by the U.S. person, if the components, part, tool or test equipment is to be used for manufacture, assembly, testing, production or modification, provided that no components, parts, tools or test equipment or the direct product of such components, parts, tools or test equipment are transferred or reexported to a country other than the United States from such subsidiary, affiliate or facility without prior authorization by BXA.

(B) For purposes of this paragraph (a)(2)(ix), U.S. person is defined as follows: an individual who is a citizen of the United States, an individual who is a lawful permanent resident as defined by 8 U.S.C. 1101(a)(2) or an individual who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). U.S. person also means any juridical person organized under the laws of the United States, or any jurisdiction within the United States (e.g., corporation, business association, partnership, society, trust, or any other entity, organization or group that is

incorporated to do business in the United States).

* * * * *

§ 740.10 [Amended]

16. Section 740.10 is amended by revising the reference to "§ 740.8(a)(2)(ii)" in paragraph (a)(2)(i) to read "§ 740.9(a)(2)(ii)".

17. Section 740.11 is amended by adding new paragraph (a)(3) to read as follows:

§ 740.11 Governments and international organizations (GOV).

* * * * *

(a) *International safeguards.* * * *

(3) No encryption items controlled for EI reasons under ECCNs 5A002, 5D002, or 5E002 may be exported under the provisions of this paragraph (a).

* * * * *

18. Section 740.14 is amended by revising paragraphs (a), (b), and (c); by adding a sentence to the end of paragraph (d); and by adding paragraph (f) to read as follows:

§ 740.14 Baggage (BAG).

(a) *Scope.* This License Exception authorizes individuals leaving the United States either temporarily (i.e., traveling) or longer-term (i.e., moving) and crew members of exporting or reexporting carriers to take to any destination, as personal baggage, the classes of commodities and software described in this section.

(b) *Eligibility.* Individuals leaving the United States may export or reexport any of the following commodities or software for personal use of the individuals or members of their immediate families traveling with them to any destination or series of destinations. Individuals leaving the United States temporarily (i.e., traveling) must bring back items exported and reexported under this License Exception unless they consume the items abroad or are otherwise authorized to dispose of them under the EAR. Crew members may export or reexport only commodities and software described in paragraphs (b)(1) and (b)(2) of this section to any destination.

(1) *Personal effects.* Usual and reasonable kinds and quantities for personal use of wearing apparel, articles of personal adornment, toilet articles, medicinal supplies, food, souvenirs, games, and similar personal effects, and their containers.

(2) *Household effects.* Usual and reasonable kinds and quantities for personal use of furniture, household effects, household furnishings, and their containers.

(3) *Vehicles.* Usual and reasonable kinds and quantities of vehicles, such as passenger cars, station wagons, trucks, trailers, motorcycles, bicycles, tricycles, perambulators, and their containers.

(4) *Tools of trade.* Usual and reasonable kinds and quantities of tools, instruments, or equipment and their containers for use in the trade, occupation, employment, vocation, or hobby of the traveler or members of the household being moved. For special provisions regarding encryption items subject to EI controls, see paragraph (f) of this section.

(c) *Limits on eligibility.* The export of any commodity or software is limited or prohibited, if the kind or quantity is in excess of the limits described in this section. In addition, the commodities or software must be:

(1) Owned by the individuals (or by members of their immediate families) or by crew members of exporting carriers on the dates they depart from the United States;

(2) Intended for and necessary and appropriate for the use of the individuals or members of their immediate families traveling with them, or by the crew members of exporting carriers;

(3) Not intended for sale or other disposal; and

(4) Not exported under a bill of lading as cargo if exported by crew members.

(d) * * * No items controlled for EI reasons may be exported or reexported as unaccompanied baggage.

* * * * *

(f) *Special provisions: encryption software subject to EI controls.* (1) Only a U.S. citizen or permanent resident as defined by 8 U.S.C. 1101(a)(20) may permanently export or reexport encryption items controlled for EI reasons under this License Exception.

(2) The U.S. citizen or permanent resident must maintain effective control of the encryption items controlled for EI reasons.

(3) The encryption items controlled for EI reasons may not be exported or reexported to Country Group E:2, Iran, Iraq, Sudan, or Syria.

19. New Supplement No. 3 is added to read as follows:

Supplement No. 3 To Part 740—Countries Eligible To Receive General Purpose Encryption Commodities and Software for Banks and Financial Institutions

Anguilla
Antigua
Argentina
Aruba
Australia
Austria
Bahamas
Barbados
Belgium
Brazil
Canada
Croatia
Denmark
Dominica
Ecuador
Finland
France
Germany
Greece
Hong Kong
Hungary
Iceland
Ireland
Italy
Japan
Kenya
Luxembourg
Monaco
Netherlands
New Zealand
Norway
Poland
Portugal
St. Kitts & Nevis
St. Vincent/Grenadines
Seychelles
Singapore
Spain
Sweden
Switzerland
Trinidad & Tobago
Turkey
Uruguay
United Kingdom

PART 742—[AMENDED]

20. Section 742.15 is amended:

a. By revising paragraph (b)(1);

b . By revising the phrase "up to 56-bit key length DES or equivalent strength" to read "56-bit DES or equivalent" in paragraph (b)(3) wherever it appears;

c.–d. By revising the phrase "The use of License Exception KMI" in the seventh sentence of paragraph (b)(3)(i) to read "Authorization to use License Exception KMI';

e. By redesignating paragraphs (b)(4) and (5) as (b)(6) and (7);

f. By adding new paragraphs (b)(4) and (b)(5); and

g. By revising newly designated paragraph (b)(6)(i) to read as follows:

§ 742.15 Encryption items.

* * * * *

(b) * * *

(1) *Certain mass-market encryption software.* (i) Consistent with E.O. 13026 of November 15, 1996 (61 FR 58767), certain encryption software that was transferred from the U.S. Munitions List to the Commerce Control List pursuant to the Presidential Memorandum of November 15, 1996 may be released from EI controls and thereby made eligible for mass market treatment after a one-time technical review. To determine eligibility for mass market

treatment, exporters must submit a classification request to BXA. 40-bit mass market encryption software using RC2 or RC4 may be eligible for a 7-day review process, and company proprietary software or 40-bit DES implementations may be eligible for 15-day processing. Refer to Supplement No. 6 to part 742 and § 748.3(b)(3) of the EAR for additional information. Note that the one-time technical review is for a determination to release encryption software in object code only unless otherwise specifically requested. Exporters requesting release of the source code should refer to paragraph (b)(3)(v)(E) of Supplement No. 6 to part 742.

(ii) If, after a one-time technical review, BXA determines that the software is released from EI controls, such software is eligible for all provisions of the EAR applicable to other software, such as License Exception TSU for mass-market software. Furthermore, for such software released from EI controls, subsequent bundling, updates, or releases consisting of or incorporating this software may be exported and reexported without a separate one-time technical review, so long as the functional encryption capacity (e.g., algorithm, key modulus) of the originally reviewed mass-market encryption software has not been modified or enhanced. However, if BXA determines that the software is not released from EI controls, a license is required for export and reexport to all destinations, except Canada, and license applications will be considered on a case-by-case basis.

(2) * * *

(3) * * *

(4) *General purpose non-recoverable encryption commodities or software of any key length for use by banks/financial institutions.* (i) Commodities and software that have already received a one-time technical review through a classification request or have been licensed for export under an Encryption Licensing Arrangement or a license are eligible for export under License Exception KMI (see § 740.8(b)(2)(iii) of the EAR) without an additional one-time technical review, providing that the export meets all the terms and conditions of License Exception KMI.

(ii) For exports not eligible under License Exception KMI, exports of general purpose non-recoverable non-voice encryption commodities or software of any key length will be permitted under an Encryption Licensing Arrangement for use by banks and financial institutions as defined in part 772 of the EAR in all destinations except Cuba, Iran, Iraq, Libya, North Korea, Syria and Sudan. No business or marketing plan is required. Applications for such commodities and software will receive favorable consideration when the end-use is limited to secure business financial communications or transactions and financial communications/ transactions between the bank and/or financial institution and its customers, and provided that there are no concerns about the country or financial end-user. No customer to customer communications or transactions are allowed. Furthermore, licenses for such exports will require the license holder to report to BXA information concerning the export such as export control classification number, number of units in the shipment, and country of ultimate destination. Note that any country or end-user prohibited to receive encryption commodities and software under a specific Encryption Licensing Arrangement is reviewed on a case-by-case basis, and may be considered by BXA for eligibility under future Encryption Licensing Arrangement requests.

(5) *Non-recoverable financial-specific encryption items of any key length.* After a one-time technical review via a classification request, non-recoverable financial-specific encryption items of any key length that are restricted by design (e.g. highly field-formatted and validation procedures, and not easily diverted to other end-uses) for financial applications will be permitted for export and reexport under License Exception KMI (see § 740.8 of the EAR). No business and marketing plan is required.

(6) *All other encryption items.* (i) *Encryption licensing arrangement.* Applicants may submit license applications for exports and reexports of certain encryption commodities and software in unlimited quantities for all destinations except Cuba, Iran, Iraq, Libya, North Korea, Syria, and Sudan. Applications will be reviewed on a case-by-case basis. If approved, encryption licensing arrangements may be valid for extended periods as requested by the applicant in block #24 on Form BXA-748P. In addition, the applicant must specify the sales territory and class(es) of end-user(s). Such licenses may require the license holder to report to BXA certain information such as ECCN, item description, quantity, and end-user name and address.

* * * * *

21. Part 742 is amended by revising Supplement Nos. 4 and 6 to read as follows:

Supplement No. 4 to Part 742—Key Escrow or Key Recoverable Products Criteria

Key Recoverable Feature

(1) The key(s) or other material/information required to decrypt ciphertext shall be accessible through a key recoverable feature.

(2) The product's cryptographic functions shall be inoperable until the key(s) or other material/information required to decrypt ciphertext is recoverable by government officials under proper legal authority and without the cooperation or knowledge of the user.

(3) The output of the product shall automatically include, in an accessible format and with a frequency of at least once every three hours, the identity of the key recovery agent(s) and information sufficient for the key recovery agent(s) to identify the key(s) or other material/information required to decrypt the ciphertext.

(4) The product's key recoverable functions shall allow access to the key(s) or other material/information needed to decrypt the ciphertext regardless of whether the product generated or received the ciphertext.

(5) The product's key recoverable functions shall allow for the recovery of all required decryption key(s) or other material/information required to decrypt ciphertext during a period of authorized access without requiring repeated presentations of access authorization to the key recovery agent(s).

Interoperability Feature

(6) The product's cryptographic functions may:

(i) Interoperate with other key recoverable products that meet these criteria, and shall not interoperate with products whose key recovery feature has been altered, bypassed, disabled, or otherwise rendered inoperative;

(ii) Send information to non-key recoverable products only when assured access is permitted to the key(s) or other material/information needed to decrypt ciphertext generated by the key recoverable product. Otherwise, key length is restricted to less than or equal to 56-bit DES or equivalent.

(iii) Receive information from non-key recoverable products with a key length restricted to less than or equal to 56-bit DES or equivalent.

Design, Implementation and Operational Assurance

(7) The product shall be resistant to efforts to disable or circumvent the attributes described in criteria one through six.

(8) The product's cryptographic function's key(s) or other material/information required to decrypt ciphertext shall be escrowed with a key recovery agent(s) (who may be a key recovery agent(s) internal to the user's organization) acceptable to BXA, pursuant to the criteria in supplement No. 5 to part 742. Since the establishment of a key management infrastructure and key recovery agents may take some time, BXA will, while the infrastructure is being built, consider exports of key recoverable encryption products which facilitate establishment of the key management infrastructure before a key recovery agent is named.

Supplement No. 6 To Part 742—Guidelines for Submitting a Classification Request for a Mass Market Software Product That Contains Encryption

Classification requests for release of certain mass market encryption software from EI controls must be submitted on Form BXA-748P, in accordance with § 748.3 of the EAR. To expedite review of the request, clearly mark the envelope "Attn.: Mass Market Encryption Software Classification Request". In Block 9: Special Purpose of the Form BXA-748P, you must insert the phrase "Mass Market Encryption Software. Failure to insert this phrase will delay processing. In addition, the Bureau of Export Administration recommends that such requests be delivered via courier service to: Bureau of Export Administration, Office of Exporter Services, Room 2705, 14th Street and Pennsylvania Ave., NW, Washington, DC 20230.

In addition, send a copy of the request and all supporting documents by Express Mail to: Attn: Mass Market Encryption Request Coordinator, P.O. Box 246, Annapolis Junction, MD 20701-0246.

(a) Requests for mass market encryption software that meet the criteria in paragraph (a)(2) of this Supplement will be processed in seven (7) working days from receipt of a properly completed request. Those requests for mass market encryption software that meet the criteria of paragraph (a)(1) of this supplement only will be processed in fifteen (15) working days from receipt of a properly completed request. When additional information is requested, the request will be processed within 15 working days of the receipt of the requested information.

(1) A mass market software product that meets all the criteria established in this paragraph will be processed in fifteen (15) working days from receipt of the properly completed request:

(i) The commodity must be mass market software. Mass market software is computer software that is available to the public via sales from stock at retail selling points by means of over-the-counter transactions, mail order transactions, or telephone call transactions;

(ii) The software must be designed for installation by the user without further substantial support by the supplier. Substantial support does not include telephone (voice only) help line services for installation or basic operation, or basic operation training provided by the supplier; and

(iii) The software includes encryption for data confidentiality.

(2) A mass market software product that meets all the criteria established in this paragraph will be processed in seven (7) working days from receipt of the properly completed request:

(i) The software meets *all* the criteria established in paragraph (a)(1)(i) through (iii) of this supplement;

(ii) The data encryption algorithm must be RC4 or RC2 with a key space no longer than 40-bits. The RC4 and RC2 algorithms are proprietary to RSA Data Security, Inc. To ensure that the subject software is properly licensed and correctly implemented, contact RSA Data Security, (415) 595-8782;

(iii) If any combination of RC4 or RC2 are used in the same software, their functionality must be separate. That is, no data can be operated sequentially on by both routines or multiply by either routine;

(iv) The software must not allow the alteration of the data encryption mechanism and its associated key spaces by the user or any other program;

(v) The key exchange used in data encryption must be:

(A) A public key algorithm with a key space less than or equal to a 512-bit modulus and/or;

(B) A symmetrical algorithm with a key space less than or equal to 64-bits; and

(vi) The software must not allow the alteration of the key management mechanism and its associated key space by the user or any other program.

(b) To submit a classification request for a product that is eligible for the seven-day handling, you must provide the following information in a cover letter to the classification request. Send the original to the Bureau of Export Administration. Send a copy of the application and all supporting documentation by Express Mail to: Attn.: Mass Market Encryption Request Coordinator, P.O. Box 246, Annapolis Junction, MD 20701-0246.

Instructions for the preparation and submission of a classification request that is eligible for seven day handling are as follows:

(1) If the software product meets the criteria in paragraph (a)(2) of this supplement, you must call the Department of Commerce on (202) 482-0092 to obtain a test vector, or submit to BXA a copy of the encryption subsystem source code. The test vector or source code must be used in the classification process to confirm that the software has properly implemented the approved encryption algorithms.

(2) Upon receipt of the test vector, the applicant must encrypt the test plain text input provided using the commodity's encryption routine (RC2 and/or RC4) with the given key value. The applicant should not pre-process the test vector by any compression or any other routine that changes its format. Place the resultant test cipher text output in hexadecimal format on an attachment to form BXA-748P.

(3) You must provide the following information in a cover letter to the classification request:

(i) Clearly state at the top of the page "Mass Market Encryption Software—7 Day Expedited Review Requested';

(ii) State that you have reviewed and determined that the software subject to the classification request meets the criteria of paragraph (a)(2) of this supplement;

(iii) State the name of the single software product being submitted for review. A separate classification request is required for each product;

(iv) State how the software has been written to preclude user modification of the encryption algorithm, key management mechanism, and key space;

(v) Provide the following information for the software product:

(A) Whether the software uses the RC2 or RC4 algorithm and how the algorithm(s) is used. If any combination of these algorithms are used in the same product, also state how the functionality of each is separated to assure that no data is operated by more than one algorithm;

(B) Pre-processing information of plaintext data before encryption (e.g. the addition of clear text header information or compression of the data);

(C) Post-processing information of cipher text data after encryption (e.g. the addition of clear text header information or packetization of the encrypted data);

(D) Whether a public key algorithm or a symmetric key algorithm is used to encrypt keys and the applicable key space;

(E) For classification requests regarding source code:

(1) Reference the applicable executable product that has already received a one-time technical review;

(2) Include whether the source code has been modified by deleting the encryption algorithm, its associated key management routine(s), and all calls to the algorithm from the source code, or by providing the encryption algorithm and associated key management routine(s) in object code with all calls to the algorithm hidden. You must provide the technical details on how you have modified the source code;

(3) Include a copy of the sections of the source code that contain the encryption algorithm, key management routines, and their related calls; and

(F) Provide any additional information which you believe would assist in the review process.

(c) Instructions for the preparation and submission of a classification request that is eligible for 15-day handling are as follows:

(1) If the software product meets only the criteria in paragraph (a)(1) of this supplement, you must prepare a classification request. Send the original to the Bureau of Export Administration. Send a copy of the application and all supporting documentation by Express Mail to: Attn.: Mass Market Encryption Request Coordinator, P.O. Box 246, Annapolis Junction, MD 20701-0246.

(2) You must provide the following information in a cover letter to the classification request:

(i) Clearly state at the top of the page "Mass Market Software and Encryption: 15-Day Expedited Review Requested';

(ii) State that you have reviewed and determined that the software subject of the classification request, meets the criteria of paragraph (a)(1) of this supplement;

(iii) State the name of the single software product being submitted for review. A separate classification request is required for each product;

(iv) State that a duplicate copy, in accordance with paragraph (c)(1) of this supplement, has been sent to the 15-day Encryption Request Coordinator; and

(v) Ensure that the information provided includes brochures or other documentation or specifications relating to the software, as well as any additional information which you believe would assist in the review process.

(3) Contact the Bureau of Export Administration on (202) 482-0092 prior to

submission of the classification to facilitate the submission of proper documentation.

PART 743—[AMENDED]

§ 743.1 [Amended]

22. Section 743.1 is amended by revising the phrase "and GOV" in paragraph (b) to read "GOV and KMI (under the provisions of § 740.8(b)(2)(ii) and (iii) only".

PART 748—[AMENDED]

23. Section 748.9 is amended by revising paragraph (a)(7) and by adding new paragraph (a)(8) to read as follows:

§ 748.9 Support documents for license applications.

(a) * * *

(7) The license application is submitted to export or reexport software or technology.

(8) The license application is submitted to export or reexport encryption items controlled under ECCNs 5A002, 5B002, 5D002 and 5E002.

* * * * *

24. Section 748.10 is amended by revising paragraph (b)(1) to read as follows:

§ 748.10 Import and End-User Certificates.

* * * * *

(b) * * *

(1) Any commodities on your license application are controlled for national security (NS) reasons, except for items controlled under ECCN 5A002 or 5B002;

* * * * *

PART 750—[AMENDED]

25. Section 750.3 is amended by revising paragraph (b)(2)(i) to read as follows:

§ 750.3 Review of license applications by BXA and other government agencies and departments.

* * * * *

(b) * * *

(2) * * *

(i) The Department of Defense is concerned primarily with items controlled for national security and regional stability reasons and with controls related to encryption items;

* * * * *

26. Section 750.7 is amended:

a. By redesignating paragraphs (c) introductory text through (c)(5) as (c)(1) introductory text through (c)(1)(v);

b. By redesignating paragraphs (c)(6) introductory text through (c)(6)(v) as (c)(1)(vi) introductory text through (c)(1)(vi)(E);

c. By redesignating paragraphs (c)(7) and (8) as (c)(1)(vii) and (viii); and

d. By adding a new paragraph (c)(2) to read as follows:

§ 750.7 Issuance of licenses.

* * * * *

(c) * * *

(2)(i) For Encryption Licensing Arrangements issued by BXA for exports and reexports of items controlled under ECCN 5A002, 5B002, and 5D002, and for encryption commodities and software previously on the U.S. Munitions List and currently authorized for export or reexport under a State Department license, distribution arrangement or any other authority of the State Department, you must by letter to BXA a request for approval of any additional country of destination.

(ii) Letters requesting changes pursuant to paragraph (c)(2)(i) of this section should be made by the license holder on company letterhead, clearly identifying the original license number and the requested change. In addition, requests for changes to State licenses or other authorizations must be accompanied by a copy of the original State license or authorization. The requested changes may not take effect until approved in writing by BXA. Send requests for changes to the following address: Office of Strategic Trade, Bureau of Export Administration, U.S. Department of Commerce, Room 2705, 14th Street and Pennsylvania Ave., NW, Washington, DC 20230, Attn: Encryption Division.

* * * * *

PART 752—[AMENDED]

27. Section 752.3 is amended by redesignating paragraphs (a)(5) through (a)(10) as (a)(6) through (a)(11) and adding a new paragraph (a)(5) to read as follows:

§ 752.3 Eligible items.

(a) * * *

(5) Items controlled for EI reasons on the CCL;

* * * * *

PART 758—[AMENDED]

28. Section 758.1 is amended by adding a new paragraph (e)(1)(i)(D) to read as follows:

§ 758.1 Export clearance requirements.

* * * * *

(e) * * *

(1) * * *

(i) * * *

(D) Exports of tools of trade under License Exception TMP or BAG.

* * * * *

PART 770—[AMENDED]

29. Section 770.2 is amended by revising the section title and adding a new paragraph (m) to read as follows:

§ 770.2 Item interpretations.

* * * * *

(m) *Interpretation 13: Encryption software controlled for EI reasons.* Encryption software controlled for EI reasons under ECCN 5D002 may be pre-loaded on a laptop and exported under the tools of trade provision of License Exception TMP or the personal use exemption under License Exception BAG, subject to the terms and conditions of such License Exceptions. This provision replaces the personal use exemption of the International Traffic and Arms Regulations (ITAR) that existed for such software prior to December 30, 1996. Neither License Exception TMP nor License Exception BAG contains a reporting requirement.

PART 772—[AMENDED]

30. Part 772 is amended by adding, in alphabetical order, new definitions for "Bank", "Effective control", "Encryption licensing arrangement", and "Financial Institution", and revising paragraph (b) under the definition of "U.S. person" to read as follows:

* * * * *

Bank. Means any of the following:

(a) Bank, savings association, credit union, bank holding company, bank or savings association service corporation, Edge Act corporation, Agreement corporation, or any insured depository institution, which is organized under the laws of the United States or any State and regulated or supervised by a Federal banking agency or a State bank supervisor; or

(b) A company organized under the laws of a foreign country and regulated or supervised by a foreign bank regulatory or supervisory authority which engages in the business of banking, including without limitation, foreign commercial banks, foreign merchant banks and other foreign institutions that engage in banking activities usual in connection with the business of banking in the countries where such foreign institutions are organized or operating; or

(c) An entity engaged in the business of providing clearing or settlement services, that is, or whose members are, regulated or supervised by a Federal banking agency, a State bank supervisor, or a foreign bank regulatory or supervisory authority; or

(d) A branch or affiliate of any of the entities listed in paragraphs (a), (b), or

(c) of this definition, regulated or supervised by a Federal banking agency, a State bank supervisor or a foreign bank regulatory or supervisory authority; or

(e) An affiliate of any of the entities listed in paragraph (a), (b), (c), or (d) of this definition, engaged solely in the business of providing data processing services to a bank or financial institution, or a branch of such an affiliate.

* * * * *

Effective control. You maintain effective control over an item when you either retain physical possession of the item, or secure the item in such an environment as a hotel safe, a bonded warehouse, or a locked or guarded exhibition facility. Retention of effective control over an item is a condition of certain temporary exports and reexports.

Encryption licensing arrangement. A license that allows the export of specified products to specified destinations in unlimited quantities. In certain cases, exports are limited to specified end-users for specified end-uses. Generally, reporting of all sales of the specified products is required at six month intervals. This includes sales made under distribution arrangements and distribution and warehousing agreements that were previously issued by the Department of State for encryption items.

* * * * *

Financial Institution. Means any of the following:

(a) A broker, dealer, government securities broker or dealer, self-regulatory organization, investment company, or investment adviser, which is regulated or supervised by the Securities and Exchange Commission or a self-regulatory organization that is registered with the Securities and Exchange Commission; or

(b) A broker, dealer, government securities broker or dealer, investment company, investment adviser, or entity that engages in securities activities that, if conducted in the United States, would be described by the definition of the term "self-regulatory organization" in the Securities Exchange Act of 1934, which is organized under the laws of a foreign country and regulated or supervised by a foreign securities authority; or

(c) A US board of trade that is designated as a contract market by the Commodity Futures Trading Commission or a futures commission merchant that is regulated or supervised by the Commodity Futures Trading Commission; or

(d) A US entity engaged primarily in the business of issuing a general purpose charge, debit, or stored value card, or a branch of, or affiliate controlled by, such an entity; or

(e) A branch or affiliate of any of the entities listed in paragraphs (a), (b), or (c) of this definition regulated or supervised by the Securities and Exchange Commission, the Commodity Futures Trading Commission, or a foreign securities authority; or

(f) An affiliate of any of the entities listed in paragraph (a), (b), (c), or (e) of this definition, engaged solely in the business of providing data processing services to one or more bank or financial institutions, or a branch of such an affiliate.

* * * * *

U.S. person. (a) * * *

(b) See also §§ 740.9 and 740.14, and parts 746 and 760 of the EAR for definitions of "U.S. person" that are specific to those parts.

* * * * *

PART 774—[AMENDED]

31. In Supplement No. 1 to part 774, Category 5—Telecommunications and Information Security is amended by revising ECCNs 5A002 and 5D002 to read as follows:

5A002 Systems, equipment, application specific "assemblies", modules or integrated circuits for "information security", and specially designed components therefor.

License Requirements

Reason for Control: NS, AT, EI.

Control(s)	Country chart
NS applies to entire entry	NS Column 1.
AT applies to entire entry	AT Column 1.

EI applies to encryption items transferred from the U.S. Munitions List to the Commerce Control List consistent with E.O. 13026 of November 15, 1996 (61 FR 58767) and pursuant to the Presidential Memorandum of that date. Refer to § 742.15 of this subchapter.

License Requirement Notes: See § 743.1 of the EAR for reporting requirements for exports of commodities controlled under 5A002 and exported under License Exceptions LVS or GOV.

License Exceptions

LVS: Yes: $500 for components and spare parts only. N/A for equipment.

GBS: N/A

CIV: N/A

List of Items Controlled

Unit: $ value

Related Controls: See also 5A992. This entry does not control: (a) "Personalized smart cards" or specially designed components therefor, with any of the following characteristics: (1) Not capable of message traffic encryption or encryption of user-supplied data or related key management functions therefor; or (2) When restricted for use in equipment or systems excluded from control under the note to 5A002.c, or under paragraphs (b) through (h) of this note. (b) Equipment containing "fixed" data compression or coding techniques; (c) Receiving equipment for radio broadcast, pay television or similar restricted audience television of the consumer type, without digital encryption and where digital decryption is limited to the video, audio or management functions; (d) Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radiocommunications systems) that are not capable of end-to-end encryption; (e) Decryption functions specially designed to allow the execution of copy-protected "software", provided the decryption functions are not user-accessible; (f) Access control equipment, such as automatic teller machines, self-service statement printers or point of sale terminals, that protects password or personal identification numbers (PIN) or similar data to prevent unauthorized access to facilities but does not allow for encryption of files or text, except as directly related to the password or PIN protection; (g). Data authentication equipment that calculates a Message Authentication Code (MAC) or similar result to ensure no alteration of text has taken place, or to authenticate users, but does not allow for encryption of data, text or other media other than that needed for the authentication; (h) Cryptographic equipment specially designed, developed or modified for use in machines for banking or money transactions, and restricted to use only in such transactions. Machines for banking or money transactions include automatic teller machines, self-service statement printers, point of sale terminals, or equipment for the encryption of interbanking transactions.

Related Definitions: For the control of global navigation satellite systems receiving equipment containing or employing decryption (i.e. GPS or GLONASS), see 7A005. *Items:*

a. Systems, equipment, application specific "assemblies", modules or integrated circuits for "information security", and specially designed components therefor:

a.1. Designed or modified to use "cryptography" employing digital techniques to ensure "information security";

a.2. Designed or modified to perform cryptoanalytic functions;

a.3. Designed or modified to use "cryptography" employing analog techniques to ensure "information security";

Note: 5A002.a.3 does not control the following:

1. Equipment using "fixed" band scrambling not exceeding 8 bands and in which the transpositions change not more frequently than once every second;

2. Equipment using "fixed" band scrambling exceeding 8 bands and in which the transpositions change not more frequently than once every ten seconds;

3. Equipment using "fixed" frequency inversion and in which the transpositions change not more frequently than once every second;

4. Facsimile equipment;

5. Restricted audience broadcast equipment; and 6. Civil television equipment;

a.4. Designed or modified to suppress the compromising emanations of information-bearing signals;

Note: 5A002.a.4 does not control equipment specially designed to suppress emanations for reasons of health and safety.

a.5. Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" or the hopping code for "frequency agility" systems;

a.6. Designed or modified to provide certified or certifiable "multilevel security" or user isolation at a level exceeding Class B2 of the Trusted Computer System Evaluation Criteria (TCSEC) or equivalent;

a.7. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion.

* * * * *

5D002 Information Security—"Software".

License Requirements

Reason for Control: NS, AT, EI

Control(s)	Country chart
NS applies to entire entry	NS Column 1.
AT applies to entire entry	AT Column 1.

EI applies to encryption items transferred from the U.S. Munitions List to the Commerce Control List consistent with E.O. 13026 of November 15, 1996 (61 FR 58767) and pursuant to the Presidential Memorandum of that date. Refer to § 742.15 of the EAR.

Note: Encryption software is controlled because of its functional capacity, and not because of any informational value of such software; such software is not accorded the same treatment under the EAR as other "software"; and for the export licensing purposes encryption software is treated under the EAR in the same manner as a commodity included in ECCN 5A002. License Exceptions for commodities are not applicable.

Note: Encryption software controlled for EI reasons under this entry remains subject to the EAR even when made publicly available in accordance with part 734 of the EAR, and it is not eligible for the General Software Note ("mass market" treatment under License Exception TSU for mass market software). After a one-time BXA review, certain encryption software may be released from EI controls and made eligible for the General Software Note treatment as well as other provisions of the EAR applicable to software. Refer to § 742.15(b)(1) of the EAR, and Supplement No. 6 to part 742 of the EAR.

License Requirement Notes: See § 743.1 of the EAR for reporting requirements for exports of software controlled under 5D002 and exported under License Exception GOV.

License Exceptions

CIV: N/A

TSR: N/A

List of Items Controlled

Unit: $ value

Related Controls: See also 5D992. This entry does not control "software" "required" for the "use" of equipment excluded from control under to 5A002 or "software" providing any of the functions of equipment excluded from control under 5A002.

Related Definitions: N/A

Items:

a. "Software" specially designed or modified for the "development", "production" or "use" of equipment or "software" controlled by 5A002, 5B002 or 5D002.

b. "Software" specially designed or modified to support "technology" controlled by 5E002.

c. Specific "software" as follows:

c.1. "Software" having the characteristics, or performing or simulating the functions of the equipment controlled by 5A002 or 5B002;

c.2. "Software" to certify "software" controlled by 5D002.c.1.

Dated: September 14, 1998.

R. Roger Majak,

Assistant Secretary for Export Administration.

[FR Doc. 98-25096 Filed 9-21-98; 8:45 am]

BILLING CODE 3510-33-P

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

24 CFR Parts 401 and 402

[Docket No. FR-4298-N-02]

RIN 2502-AH09

Notice of Public Meetings Multifamily Housing Mortgage and Housing Assistance Restructuring (Mark-to-Market) Program

AGENCY: Office of the Assistant Secretary for Housing—Federal Housing Commissioner, HUD.

ACTION: Notice of public forums.

SUMMARY: On September 11, 1998 (63 FR 48925), the Department published in the **Federal Register** an interim rule implementing the Mark-to-Market Program. The Program was enacted by the Multifamily Assisted Housing Reform and Affordability Act of 1997 (MAHRA). The purpose of the program is to preserve low-income rental housing affordability while reducing the long-term costs of Federal rental assistance, including project-based assistance, and minimizing the adverse effect on the FHA insurance funds. The authorizing statute provides that before publishing the final rule HUD is to conduct at least three public forums at which organizations representing various groups identified in the statute may express views concerning HUD's proposed disposition of recommendations from those groups. This notice announces the time and places for these public forums.

DATES: The public forums will be held on Thursday, October 1, 1998, from 1 p.m. to 7:30 p.m. local time.

ADDRESSES: The public forums will be held at the following three locations:

Midland Hotel (Adams Room), 175 West Adams, Chicago, Illinois

Holiday Inn Golden Gateway, 1500 Van Ness Avenue, San Francisco, California

The College of Insurance, 101 Murray Street, New York, New York.

FOR FURTHER INFORMATION CONTACT: Leslie Breden, (202) 708-6423, ext. 5603. For hearing- and speech-impaired persons, this number may be accessed via TTY by calling the Federal Information Relay Service at 1-800-877-8339. For registration information call 1-800-685-8470, the Multifamily Housing Clearinghouse, (fax) (301)-519-5161. (Except for the 800 numbers, these are not toll-free numbers.) Additional information is available on HUD's Internet web site, at http://www.hud.gov/fha/mfh/pre/premenu.html.

SUPPLEMENTARY INFORMATION:

What Will Be Discussed at the Forums?

Section 522(a)(3)(A) of MAHRA directed HUD to seek recommendations on implementing the participating administrative entity selection criteria (see section 513(b) of MAHRA and § 401.201 of the interim rule) and on mandatory renewal of project-based assistance (see section 515(c)(1) of MAHRA and § 401.420 of the interim rule). In accordance with section 513(a)(3)(A), HUD has received recommendations from at least the following organizations: State housing finance agencies and local housing agencies; other potential participating administering entities; tenants; owners and managers of eligible multifamily housing projects; States and units of general local government; and qualified mortgagees. The recommendations covered the scope of the interim rule.

In accordance with section 522(a)(3)(B) of MAHRA, HUD is holding these public forums to provide participants with an opportunity to express their views on § 401.201 and § 401.420 of the interim rule. HUD will not be making any presentations at these forums. The purpose of these forums is for HUD to listen and record the comments of the forum participants for consideration in drafting the final rule.

How Can I Register for a Forum?

You can get registration information through HUD's portfolio reengineering

#1 pg 19.6

William A. Root
4024 Franklin Street
Kensington MD 20895
Tel. & FAX 301 942 6720

October 6, 1998

Nancy Crowe, Regulatory Policy Division
Bureau of Export Administration, Department of Commerce
P. O. Box 273, Washington DC 20044

Re: Encryption Regulations - Interim Rule of September 22, 1998

Dear Ms. Crowe:

The following comments are limited to anomalies or inconsistencies related to the subject interim rule and do not imply either concurrence or non-concurrence with the substance of that rule. Moreover, they do not repeat anomalies or inconsistencies related to other aspects of encryption regulations brought to BXA's attention in my letters of December 12, 1996, January 2, 1997, February 11, 1997, August 27, 1997, or March 9, 1998.

1. Mass market encryption software Revised 742.15(b)(1)(i), 742.15(b)(1)(ii) except for the last sentence, and 742 Supplement 6 specify conditions under which License Exception TSU for mass market software is applicable to encryption software. Unchanged 740.13(d)(2), which reads in its entirety:

> This (TSU mass market software) License Exception is not available for key escrow encryption software controlled by 5D002.c.1,

is, therefore, misleading. 742.15(b)(1) conditions for TSU eligibility should be moved to 740.13(d)(2) and 742 Supplement 6 should be moved to become a Supplement to part 740.

742 Supplement 6 first paragraph refers to Office of Exporter Services in Room 2705, whereas 730.8(c) and 748.2(a) refer to Exporter Counseling Division in Room 1099D.

742 Supplement 6 (a)(2)(iii) is garbled. Perhaps it should read:

> If any combination of RC4 or RC2 is used, no data can be operated on sequentially by both routines nor be multiplied by either routine.

2. License Exception KMI

a. "And" vs. "or" The interim rule revision to 740.8(b)(2) uses "and" rather than "or" to link "commodities and software" and to link "5A002 and 5D002," thus indicating, probably inadvertently, that KMI may be used only for transactions involving both commodities and software.

b. Wassenaar reporting 740.8(b)(2)(ii)(B) last sentence and (b)(2)(iii)(D) last sentence specify 743.1 Wassenaar reporting requirements for KMI shipments, as does the revision to 743.1(b). However, CCL listings under License Requirement Notes list only License Exceptions LVS and GOV as requiring such 5A002 reporting and only GOV as requiring such 5D002 reporting.

Wassenaar may have dropped the COCOM bank and financial institution encryption exception inadvertently, just as the U.S. did in connection with the EAR reform. In any event, it would be consistent with the interim rule for the U.S. to seek a conforming Wassenaar amendment, so that 743 reporting would not have to be required for such KMI exports.

c. License Exception vs. licensing policy Unchanged 742.15(b)(2) and (b)(3), new 742.15(b)(4)(i) and (b)(5), revised 742 Supplement 4, and unchanged 742 Supplement 5 concern conditions for License Exception KMI and, therefore, should be moved to the KMI section 740.8 and to part 740 Supplements, rather than be retained in licensing policy part 742.

d. Countries eligible to receive general purpose encryption commodities and software for banks and financial institutions

New Supplement No. 3 to Part 740 creates a substantial burden on both exporters and the government by establishing a new country group which, for no reason stated in the *Federal Register*, differs substantially from all former groups. It is understood that this new country group consists of members of a financial action Task Force, or countries agreeing to comparable conditions, and that the list is not final and could be lengthened. Errors identified in the following anomalies should be remedied immediately and it is hoped that other of these anomalies will be remedied in the near future by obtaining the likely requisite financial action cooperation of more countries:

Four Computer Tier 1 countries are omitted, as follows:
- Holy See (included in Italy per 744 Supplement 3; listed as Vatican City in the Country Chart)
- Liechtenstein (exports to Switzerland may be reexported to Liechtenstein without a license per 740.16(g))
- Mexico (NAFTA member)
- San Marino (included in Italy per 744 Supplement 3)

Seventeen Computer Tier 2 countries are listed, including eleven having no other special cooperative relationship with the United States, whereas the following four long-standing cooperating countries and 88 others are omitted:
- Czech Republic (member of NATO, Wassenaar, AG, and NSG)
- South Korea (member of Wassenaar, AG, and NSG and cooperating country per 740.11(b)(3)(ii))
- Slovakia (member of Wassenaar, AG and NSG)
- Taiwan (cooperating country per 740.11(b)(3)(ii))
- 81 others never before singled out for special treatment of any sort and previously indistinguishable from 11 of the 17 listed
- seven which, since their removal from the nuclear non-proliferation special country list, were also indistinguishable from the 11 listed, namely: Algeria, Andorra, Angola, Comoros, Djibouti, Micronesia, and Vanuatu

The one Computer Tier 3 country listed, Croatia, is not otherwise a cooperating country, whereas the following four Computer Tier 3 countries, which do cooperate in other fora, are omitted:
- Bulgaria (Wassenaar and NSG)
- Romania (Wassenaar, AG, and NSG)
- Russia (Wassenaar, MTCR, and NSG)
- Ukraine (Wassenaar)
-

Two listed countries, Anguilla and Aruba, are not named in the Country Chart in 738 Supplement 1. They should receive the licensing treatment accorded the United Kingdom and The Netherlands, respectively, pursuant to 738.3(b).

e. Definition of "bank" In paragraph (a) of the new definition of "bank" in part 772, "Agreement corporation" makes no sense. Based on an earlier draft, perhaps corporation having an agreement under section 25 of the

Federal Reserve Act (12 U.S.C. 611) is meant.

Paragraph (c) would be easier to read if the comma before "that is" were deleted.

3. *De minimis*

Interim rule revisions to 732.2(d), 732.3(e)(2), and 734.4(b)(2) clarify that *de minimis* exclusions from "subject to the EAR" do not apply to EI items controlled by ECCN 5E002 as well as to EI items controlled by ECCN 5A002 and ECCN 5D002. 732.2(d) and 732.3(e)(2) state that *de minimis* provisions do not apply to these EI items, whereas 734.4(b)(2) states that certain mass market encryption software may become eligible for *de minimis* after a one-time BXA review per 742.15(b)(1). However, after such a positive one-time BXA review, software is released from control whether or not it is *de minimis*.

EI technology and software could be made eligible for *de minimis* with no loss of control, because, pursuant to 734 Supplement 2 (b), a one-time report to BXA is a pre-requisite for all *de minimis* technology and software.

4. Electronic acknowledgments or assurances

The interim rule revision to 734.2(b)(9)(ii) adds the following sentence:

> BXA will consider acknowledgments in electronic form provided that they are adequate to assure legal undertakings similar to written acknowledgments.

An exporter reasonably assumes that an electronic acknowledgment is as legally adequate as a non-electronic written acknowledgment unless the EAR specifies otherwise. Neither a non-electronic nor an electronic acknowledgment could overcome inadequacies caused by the laws or regulations of the recipient's country blocking the extraterritorial reach of U.S. export controls. The EAR should cite any conditions which would make an electronic acknowledgment inadequate under U.S. laws and regulations.

The interim rule revision of 740.6(a)(3) states that the required TSR assurance may be in the form of any written communication from the importer "including communications via facsimile." Unlike 734.2(b)(9)(ii), this indicates that an electronic facsimile communication is a form of written communication. It also does not rule out the possibility that other forms of electronic communication, such as email, are also written communications.

If there is an intended implication that an electronic communication is adequate in the contexts of 740.6(a)(3) and 734.2(b)(9)(ii) only if the importer's signature is reproduced, this should be stated explicitly.

5. Limited value shipments

a. Support previous export The interim rule statement in 740.3(d)(5) that 5A002 components or spare parts exported under License Exception LVS must be destined to support an item previously authorized for export is not repeated in the CCL listing of 5A002, where an exporter would expect to find a restriction applicable to only one ECCN.

b. Spare parts vs. specially designed components The references to "components or spare parts" in 740.3(d)(5) and to "components and spare parts" in the LVS line of the CCL listing of 5A002 are inconsistent with the control text of 5A002, which assumes that spare parts are included

in the expression "specially designed components."

c. Software vs. commodities The ITAR provision on which 5A002 LVS eligibility is based, 22 CFR 123.16(b)(2), applies to software as well as to commodities, since ITAR defines "defense article" to include "technical data," defines "technical data" to include software, and defines "component" as an "item" and "part" as an "element," i.e., terminology not limited to commodities. However, the new encryption LVS eligibility applies only to commodities (5A002) and does not apply to software (5D002).

d. Encryption vs. other items 22 CFR 123.16(b)(2) applies generally to defense articles whereas the new LVS eligibility patterned on that ITAR provision applies only to encryption and does not apply generally to CCL items, or even to other CCL items which have been transferred from the U.S. Munitions List.

6. Effective control and controlled-in-fact

The definition of "effective control," referred to in revised 740.9(a)(2)(i) concerning tools of trade and newly added to 772, is drafted so as to apply to this expression wherever it appears in the EAR (reference in the definition to its applicability to certain temporary exports and reexports does not make it otherwise inapplicable). However, the new definition differs from the definition of "effective control" contained in 772 for purposes of the Special Comprehensive License (SCL).

On the other hand, "effective control" does not appear in EAR provisions concerning the SCL. Instead, "controlled-in-fact" is used in 752.5(b)(2)(i)(B) (twice) and in 752 Supplement 3 Block 7(ii) item (b) and the part 772 definition of "controlled-in-fact" for SCL purposes differs markedly from both of the part 772 "effective control" definitions. This situation arose because reg reform combined various special licenses into one SCL; the SCL picked up the old distribution license "controlled-in-fact" term in part 752 and its definition in part 772; and part 772 also picked up the old service supply procedure "effective control" definition even though that term was not picked up in part 752 (the old special chemical license different definition of "effective control" was not picked up in the reg reform, in either 752 or 772). The "controlled-in-fact" definition is far clearer than any of the "effective control" definitions in describing whether one entity in fact controls another entity.

New 740.9(a)(2)(ix), like 22 CFR 123.16(b)(9) after which it was patterned, refers to a subsidiary, affiliate or facility that is "controlled" by a U.S. person, without defining "controlled."

The new 772 definition of "effective control" would logically apply to the use of those words in new 740.14(f)(2), which conditions encryption software eligible for License Exception BAG.

Terms which are defined in part 772 are normally put in quotation marks in the relevant parts of the EAR, e.g., "effective control" appears in quotation marks in 740.9(a)(2)(viii)(A)(1) concerning news media. However, "effective control" in the operative portion of 740.9(a)(2)(i) and in 740.14(f)(2) and "controlled-in-fact" in all three places where it is used in part 752 are not in quotation marks.

#1 pg 5&6

To resolve these anomalies:

- "effective control" should be put in quotation marks the first place it appears in newly revised 740.9(a)(2)(i) and in 740.14(f)(2);
- the new definition of "effective control" in part 772 should be revised to insert at the beginning "For purposes of the tools of trade and news media portions of License Exception TMP and the encryption software portion of License Exception BAG," and to delete at the end "Retention of effective control over an item is a condition of certain temporary exports and reexports";
- the "effective control" definition for SCL purposes should be deleted;
- "controlled-in-fact" as used in 752 should be put in quotation marks;
- "controlled" in 740.9(a)(2)(ix) should be changed to "controlled-in-fact' (in quotation marks); and
- in the "controlled-in-fact" definition in 772 after "For purposes of the Special Comprehensive License (part 752 of the EAR)" the following should be inserted "and of the portion of License Exception TMP described in 740.9(a)(2)(ix)" (also see point 7 below, which questions inclusion of this provision in TMP).

7. Temporary vs. permanent exports to subsidiaries New 740.9(a)(2)(ix) and the ITAR provision on which it is based, 22 CFR 123.16(b)(9), use the word "temporary"; but both provisions describe permanent exports, since there is no requirement ever to return qualifying items to the country from which they were exported. It appears that 740.9(a)(2)(ix) should be moved from License Exception TMP to become exceptions to the definitions of "export" and "reexport" in 734.2 or 772.

8. Direct product New 740.9(a)(2)(ix) conditions the "temporary exports to a U.S. subsidiary, affiliate or facility in Country Group B" portion of License Exception TMP on no transfer or reexport other than to the United States of the direct product of the exported components, parts, tools or test equipment. However, pursuant to 736.2(b)(3), direct product controls apply only to the foreign-produced direct product of technology and software and only to exports and reexports to Cuba, North Korea, Libya, and countries in Country Group D:1.

9. Reexports

a. Tools of trade The new provision in 740.9(a)(2)(i) that tools of trade may accompany the individual or be exported after departure of the individual applies only to individuals departing from the United States, thereby leaving in doubt whether this rule also applies to reexports, which are also eligible for this portion of License Exceptions TMP.

b. Subsidiaries The new provision in 740.9(a)(2)(ix) perhaps inadvertently omits authorization of reexports. If reexports were authorized the exception from the prohibition against transfers or reexports should be expanded to include the country from which the reexport took place.

c. Baggage Revised 740.14 clarifies that License Exception BAG applies to longer-term moving but retention of the phrase "leaving the United States" appears, probably inadvertently, to preclude use of BAG by persons moving back to the United States or by any person whose travels or moves did not originate in the United States.

Interim rule addition of "or other disposal" after "Not intended for sale" in 740.14(c)(3) is probably intended to preclude transfers not

involving a sale. However, it would also, probably inadvertently, make items intended for consumption or destruction by the traveler ineligible for License Exception BAG.

10. Encryption software eligibility for License Exception BAG Revised 740.14(b)(4), new last sentence of 740.14(d), new 740.14(f), and new 770.2(m) provide that tools of trade encryption software may be exported under License Exception BAG. However, unchanged 740.14(d)(2) states that this License Exception is not available for encryption software controlled for "EI" reasons under ECCN 5D002.

11. License changes The word "submit" was inadvertently omitted from revised 750.7(c)(2)(i).

12. SED exemption for baggage The new 758.1(e)(1)(i)(D) SED exemption for items shipped under License Exception BAG is limited to tools of trade. However, FTSR 30.56(a), as reproduced in 786A Supplement 1 dated March 1994, records an SED exemption for other items eligible for License Exception BAG and 30.56(b) contains one condition on eligibility for the tools of trade baggage SED exemption which is not in 740.14 or 758.1(e)(1)(i)(D), namely, "shall be in his possession at the time of or prior to his departure from the United States for a foreign country."

13. Encryption software license exceptions The interim rule clarifies, in parts 740, 742.15, and 770.2, the applicability to encryption software of License Exceptions KMI, TMP tools of trade, GOV official use of U.S. Government personnel and agencies, TSU mass market software, and BAG accompanied baggage. In addition, the lack of an EI exclusion for RPL servicing and replacement implies applicability of that License Exception to EI software. However, the interim rule does not revise the following statements in the first Note under 5D002 in part 774, which provide, in effect, that all License Exceptions are inapplicable to encryption software:

> ... encryption software is treated under the EAR in the same manner as a commodity ... License Exceptions for commodities are not applicable.

14. Definition of "U.S. person"

a. Cross references The revised definition of "U.S. person" in part 772 adds 740.9 and 740.14 to the list where definitions of this term specific to other EAR parts may be found. However, it omits a reference to 744.9(b), where a definition relevant to technical assistance with respect to encryption items may be found. Greater specificity would be more user-friendly, i.e., by citing 740.9(a)(2)(ix)(B), 740.14(e)(1), 746.9(b)(3)(ii), and 760.1(b) instead of 740.9, 740.14, 746, and 760.

b. Content It seems unlikely that so many different definitions are necessary. The one in 760.1(b) is the most precise.

Sincerely yours,

William A. Root

William A. Root

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

#3 pg 1 of 4

Microsoft

VIA FAX

November 6, 1998

Ms. Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
P.O. Box 273
Washington, D.C. 20044

Re: Microsoft Comments on September 22, 1998 Interim Rule on Encryption Export Controls

Dear Ms. Crowe:

On behalf of Microsoft Corporation, I hereby submit comments on the interim final rule published in 63 Fed. Reg. 50516 (Sept. 22, 1998) (hereinafter the "Rule"). As you may recall, Microsoft submitted detailed comments to your department on a draft version of this regulation dated July 1997. The final version of the regulations includes several changes and improvements based in part on these and other comments, for which we thank you. Indeed, the rule is a vast improvement on the earlier draft, which demonstrates the sensibility of BXA soliciting comments on the rule in draft form. We have several additional comments, however, which are provided in the order of the regulations for your convenience:

EAR Sec. 740.8

Sec. 740.8 describes License Exception KMI, which applies to key recovery and key escrow items. As amended by the Rule, however, this section now includes several categories of non-recoverable encryption software. We believe that this is confusing to exporters and especially to their customers, who might be misled into thinking that products exported under this provision embody a key recovery scheme, which would inhibit the marketability of non-recoverable U.S. products. This confusion will be increased as the categories of acceptable non-recovery items expand. We therefore strongly recommend that you move the non-recovery items (Sec. 740.8(b)(2)(i), (ii), and (iii)) to a new license exception, such as proposed License Exception ENC.

EAR Sec. 740.8(b)(2)(ii) and the Longstanding "Money and Banking" Exception

The EAR has long permitted exporters to self-classify commodities and software that are designed and limited for use in banking or money transactions (5A002/Related Controls (h) and by reference 5D002, which also existed as exceptions to encryption controls under the International Traffic in Arms Regulations). It is unclear at best what the difference is between items falling under these longstanding "money and banking" exceptions described in 5A002/5D002 and those falling under this new Section 740.8(b)(2)(ii) for financial-specific encryption products. Financial-specific encryption items should continue to be reviewed via Advisory Opinions as an option, not on a mandatory basis. The new License Exception KMI provision calls for mandatory one-time review of the types of products that have

for years been interpreted by the Department of State and the National Security Agency as falling under the provisions of the "money and banking exception." In order to be clear and consistent, and to avoid unnecessary requests for classifications, BXA should move all non-recoverable, financial-specific items to ECCN 5A992/5D992 categories. This could be done via a new definition or a new interpretation. A new definition for "financial-specific" could include detailed language describing the criteria for eligibility (e.g., "highly field formatted with validation procedures and not easily diverted to other end-uses" and/or "to secure financial communications/transactions for end-uses such as financial transfers or electronic commerce"), or the classification could be clarified in a new interpretation. It would be important to make clear in the definition that the concept of "securing financial communications/transactions" includes all forms of communication, such as e-mail.

EAR Sec 740.8(b)(2)(iii)

In Sec. 740.8(b)(2)(iii), License Exception KMI permits the export or re-export of general purpose non-recoverable encryption commodities or software of any key length for use by banks/financial institutions (after a one time technical review or prior issuance of a license). Such exports are subject to Wassenaar reporting. It should be permissible for an exporter of these commodities or software to engage in indirect bulk distribution via non-financial intermediate consignees, such as Systems Integrators or Value Added Resellers, and not be restricted to making individual exports directly to eligible banks and financial institutions. The typical business pattern in this area is for exporter to make bulk shipments of commodities or software to overseas distributors, who over time provide individual units from stock to eligible end-users in accordance with KMI. As with other license exceptions, the exporter and their foreign intermediate consignees are responsible for adhering to the terms and conditions of License Exception KMI. The regulation should be clarified to insure that exporters are not prohibited from export or re-export of eligible commodities or software under KMI to non-bank, non-financial intermediate consignees for re-distribution to eligible end-users. Indirect bulk distribution via non-financial intermediate consignees would appear not to impact Wassenaar reporting - the exporter would submit a Wassenaar report to BXA in accordance with Sec 743.1, giving the ECCN and paragraph reference for the software provided to the foreign intermediate consignee, number of units in the shipment, and country of ultimate destination (as known at the time of export).

EAR Sec. 740 - Supplement No. 3

The limited list of countries whose banks and financial institutions are authorized to receive exports is an unwarranted roll back of authority granted to export to banks and financial institutions in previously issued ELAs by the State as well as the Commerce Department. This puts exporters without existing ELAs at a disadvantage vis-à-vis those with ELAs, and subjects new products to tighter restrictions than older products even if the encryption used in the product is the same. We understand that this policy decision was a result of a compromise among different agencies. Nevertheless, this rollback undercuts the credibility of the Administration's liberalization of encryption policy.

At minimum, the exporting community deserves to be told in advance which countries will be excluded from Encryption Licensing Arrangements to banks and financial institutions in destinations outside said 44 countries (except the seven embargoed and terrorist supporting countries). It is inappropriate not to list countries to which the U.S. will not allow such exports due to money laundering concerns. It appears that the Administration has put diplomatic concerns of not offending countries that do not adequately restrict money laundering ahead of the needs of exporters. Even with advance notification, this rollback of authorization to export products to banks in closely allied countries such as Mexico and other Latin American and Caribbean countries is unwarranted, especially given that that banks in those countries may continue to receive products with the same encryption under existing ELAs issued to US vendors prior to these regulations.

In addition, while we understand that BXA intended to put branches of U.S. banks outside the U.S. on the same footing with branches of foreign banks, the fact that the U.S. is not included in this Supplement 3 list has created uncertainty about whether we can rely solely on the definition of "Bank" to achieve that result. We understand that Jim Lewis has given verbal advice to the effect that exporters may ship general purpose encryption items to branches of U.S. banks anywhere, as stated in Commerce Secretary Daley's press release of July 7, 1998. But this is such a fundamental omission that BXA should put this advice in writing on its web page, both the guidance as well as correct the rule by adding the U.S. to Supplement 3, thereby providing exporters greater certainty on this issue.

Part 772 – Definition of "Bank"

As drafted in the interim regulations, Subparagraph (e) of this definition appears to cover only those "affiliates" whose sole and exclusive business is providing data processing services to banks or financial institutions. In our experience, many entities that provide data processing services to banks and financial institutions also provide similar services to non-financial organizations. In addition, these "affiliates" may also develop data processing services and products. Therefore, we suggest that the paragraph be revised to read: "An affiliate of any of the entities listed in paragraphs (a), (b), (c) or (d) of this definition, when it is engaged by the entity for the purpose of developing or providing data processing services or products to a bank or financial institution, or a branch of such an affiliate."

Part 772 – Definition of "Effective control"

We are concerned that identifying specific security measures, such as hotel safes, makes the definition more confusing and unnecessarily restrictive. For example, to protect sensitive business information, many business travelers take precautions to protect the software and data on laptops, such as password protecting "boot up" or encrypting the contents of the hard drive. Requiring the use of a safe or bonded warehouse is inconsistent with modern business practices and would effectively gut the laptop exemption for nearly all business travelers. We believe that the intent of "effective control" is to require the exporter to take positive steps to protect the items being temporarily exported or re-exported. Trying to define the many ways in which an item might be secured is probably unrealistic.

Therefore, we suggest that the definition be simplified as follows: "You maintain effective control over an item when you retain physical possession of the item or take other steps to secure the item." Alternatively, we suggest that BXA consider not defining the term at all.

Part 772 – Definition of "Financial Institution"

Comment 1: The definition should include clearing or settlement services as mentioned in subparagraph (c)of the definition of "Bank."

Comment 2: We suggest that subparagraph (f) be revised in a manner similar to the suggested revision for subparagraph (e) in the definition of "Bank."

Part 774 – CCL Categories 5A002 and 5D002

It would be extremely helpful to create different classification categories for items removed from EI controls. It is very confusing for many exporters whose systems are geared to control items by their ECCNs to discriminate between ECCN 5D002.c.1 EI controlled items that require a license to every destination and 5D002.c.1 non-EI controlled items that are eligible for export to all but seven countries under License Exception TSU. The "classification" appears meaningless. We assume that Customs has similar problems.

The following statement should be eliminated from the first note to ECCN 5D002: "License Exceptions for commodities are not applicable." This is confusing and not necessary, as many license exceptions that are generally used primarily for commodities have been considered by BXA to be applicable to encryption software (TMP, BAG, GOV, etc.).

We appreciate the opportunity to comment of these regulations. Please do not hesitate to contact the undersigned if you have questions or wish to discuss any of these comments.

Respectfully submitted,

Ira S. Rubinstein
Senior Corporate Attorney

cc: Mr. James Lewis
Ms. Patricia Sefcik

INVESTMENT COMPANY INSTITUTE

November 6, 1998

Ms. Nancy Crowe
Export Policy Analyst
Regulatory Policy Division
Bureau of Export Administration
U.S. Department of Commerce
14th & Pennsylvania Avenues, NW
Room 2705
Washington, D.C. 20230

Re: Encryption Export Regulation – Interim Rule

Dear Ms. Crowe:

The Investment Company Institute[1] (the "Institute") appreciates the opportunity to comment on the Department of Commerce's interim rule on encryption exports.[2] The Interim Rule would, among other things, implement new licensing policies for general purpose non-recoverable, non-voice encryption commodities or software of any key length for distribution to banks and financial institutions in specified countries.

The Institute supports the Interim Rule because it should facilitate secure communications between our members' domestic offices and various overseas entities that play an integral role in the global investment management business. In particular, we are pleased that the Department has included in the definition of "financial institution" most of the key entities involved in the investment management industry, including investment companies (often referred to as "mutual funds"), investment advisers, brokers, dealers, and their branches or affiliates, which are regulated or supervised by the Securities and Exchange Commission, the Commodity Futures Trading Commission, or a foreign securities authority. Our comments below seek clarification that the definition of "financial institution" includes mutual fund transfer agents and administrators, entities that are not specifically identified in the Interim Rule but that are just as vital to the operation of a mutual fund as the other entities mentioned in the rule. We also seek clarification of the circumstances in which U.S. exporters may export directly to retail customers of a bank or financial institution under the Interim Rule.

---

[1] The Investment Company Institute is the national association of the American investment company industry. Its membership includes 7,335 open-end investment companies ("mutual funds"), 451 closed-end investment companies and 9 sponsors of unit investment trusts. Its mutual fund members have assets of about $4.837 trillion, accounting for approximately 95% of total industry assets, and have over 62 million individual shareholders. Many of the Institute's investment adviser members render investment advice to both investment companies and other clients. In addition, the Institute's membership includes 497 associate members that render investment management services exclusively to non-investment company clients. A substantial portion of the total assets managed by registered investment advisers are managed by these Institute members and associate members.

[2] *Encryption Items*, Department of Commerce, Bureau of Export Administration, 63 Fed. Reg. 50516 (Sept. 22, 1998) (the "Interim Rule").

Mutual Fund Transfer Agents and Administrators

As noted above, the transfer agent function is an important function for mutual fund operations. Mutual fund transfer agents maintain records of shareholder accounts, which reflect daily investor purchases, redemptions, and account balances. These transfer agents typically serve as dividend disbursing agents and their duties as such involve calculating dividends, authorizing payment by the custodian, and maintaining dividend payment records. In addition, transfer agents prepare and mail to shareholders periodic account statements, federal income tax information, and other shareholder notices. In many cases, transfer agents prepare and mail on behalf of the mutual fund and its principal underwriter statements confirming transactions and reflecting share balances. Moreover, transfer agents often maintain customer service departments that respond to telephone and mail inquiries concerning the status of shareholder accounts.

Equally important to mutual fund operations is the administrative function. A mutual fund administrator provides administrative services to a fund. These services, which often are performed by the fund's investment adviser, include overseeing the performance of other companies that provide services to the fund, as well as assuring that the fund's operations comply with applicable regulatory requirements. Administrators typically provide office space, equipment, personnel, and facilities; provide general accounting services; and help establish and maintain compliance procedures and internal controls. Often, they assume responsibility for preparing and filing various regulatory, shareholder, and other reports.

Many U.S. firms sponsor and manage funds that are organized offshore for sale to offshore residents. While the management companies for these funds often are located in the U.S., fund administration and shareholder servicing may be provided by affiliated or third-party entities located outside the U.S. Institute members that are active in sponsoring and/or managing offshore funds have a strong interest in being able to use secure communications between their domestic offices and the overseas entities (including transfer agents and administrators) that service their offshore funds.

Although not specifically identified in the Interim Rule, mutual fund transfer agents and administrators ostensibly are included within the scope of the rule to the extent they are affiliates or branches of the entities named in the rule. It is unclear, however, whether these entities are covered when their affiliation with a mutual fund is based on a third-party, arm's length contractual relationship as opposed to, for example, when they are part of the same financial services organization as the mutual funds' investment adviser.

We believe that because of the essential functions performed by transfer agents and administrators on behalf of the mutual funds they serve, their inclusion in the Interim Rule is intended. To further clarify this intention, and to ensure the inclusion of *all* relevant entities that play key roles in the operation of mutual funds, we recommend that mutual fund transfer agents and administrators be specifically identified among the entities delineated in Part 772, subparagraphs (a) and (b) of the definition of "financial institution," or, alternatively, that the term "affiliate" in subparagraph (e) of that definition be defined to include entities that are under contract to an investment company or an investment adviser to provide transfer agent or

administrative services. In the event that neither of these suggestions can be accommodated, we ask that this clarification be noted in the explanatory material accompanying the final rule.

Direct Exports to Retail Customers of Banks or Financial Institutions

The Institute also seeks clarification of the circumstances in which U.S. exporters may export directly to the retail customers of a bank or financial institution under the Interim Rule. As drafted, the Interim Rule appears to permit U.S. encryption exports to qualifying banks and financial institutions to secure financial communications/transactions with and between those entities and their customers. It is anomalous that U.S. exporters do not appear to have the same flexibility to export encryption to the overseas retail customers of U.S. banks and financial institutions, even when the encryption products do not permit customer-to-customer communications. To clarify the regulations in this regard, we recommend amending the Interim Rule (specifically, 15 CFR Part 740.8(2)(iii)) to permit distribution to overseas retail customers of U.S. banks and financial institutions of general-purpose unrecoverable encryption so long as the products are not useable for customer-to-customer communications/transactions.

* * * * *

The Institute appreciates the opportunity to comment on the Interim Rule. Any questions on our comments may be directed to the undersigned at (202) 326-5822 or to Barry E. Simmons at (202) 326-5923.

Sincerely,

Frances M. Stadler

Frances M. Stadler
Deputy Senior Counsel

cc: James Lewis
Director
Office of Strategic Trade and Foreign Policy Controls

#5 98183

BROOX W. PETERSON
Senior Vice President &
Assistant General Counsel

VISA
WORLDWIDE PARTNER

November 6, 1998

VIA MESSENGER

RECEIVED
1998 NOV 6 P 1:15
EOA/ESS

Ms. Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
P.O. Box 273
Washington, DC 20044

Re: Export Administration Regulations: Interim Rule
Docket No. 980911233-8233-01

Dear Ms. Crowe:

Visa International[1] appreciates this opportunity to comment on the Department of Commerce's interim rule (the "Interim Rule") amending the Export Administration Regulations (the "EAR") to clarify the controls on the export and reexport of encryption items controlled for "EI" reasons on the Commerce Control List, published in the September 22, 1998 Federal Register (63 Fed. Reg. 50516).

The Visa payments system is the largest consumer payments system in the world. Visa is a joint venture comprised of more than 21,000 financial institution members from around the world that have issued over 640 million Visa payment cards, which are accepted at more than 14 million merchant locations and at over 400,000 automated teller machines worldwide. Visa - which provides transaction authorization, clearing and settlement, and risk management services to financial institution members - supports more than $1 trillion in Visa-related payment transactions annually throughout the world. At peak volume, Visa systems process over 2,400 card related transactions per second.

[1] VISA International is a membership organization comprised of financial institutions throughout the world licensed to use the Visa service marks in connection with payment systems. For purposes of this letter, the term Visa refers to Visa International.

VISA INTERNATIONAL
Post Office Box 8999
San Francisco, CA 94128-8999
U.S.A.

Phone 650 432 3161
Fax 650 432 2145
E-mail peterson@visa.com

The secure and smooth functioning of international payment systems such as the Visa system is of critical importance to financial institutions and their customers, as well as the overall world economy. Visa and its member financial institutions around the world must be able to utilize appropriate current and future technologies to secure this payments system.

Towards this end, Visa supports the provisions of Section 740.8 of the Interim Rule that permit, after a one-time technical review, the export and reexport of non-recoverable financial-specific encryption software and commodities of any key length, that are restricted by design for financial applications to secure financial transactions, for end-uses such as financial transfers or electronic commerce. Visa also supports the provisions of Section 740.8 of the Interim Rule that permit, after a one-time review, exports and reexports of general purpose non-recoverable non-voice encryption commodities or software of any key length for distribution to banks and financial institutions located in certain specified countries, provided the end-use is limited to secure business financial communications or transactions or financial communications/ transactions between the bank or financial institution and its customer.

Visa is particularly pleased that, for purposes of these provisions of Section 740.8, the definitions of the terms "bank" and "financial institution" are sufficiently broad to include Visa and its financial institution members. In particular, the definition of the term "bank" includes an entity such as Visa engaged in the business of providing clearing or settlement services, or whose members are regulated or supervised by a U.S. federal or state bank regulator or supervisor or a foreign bank regulatory or supervisory authority. This definition also would include Visa member banks, savings associations, credit unions, bank holding companies, bank or savings association service companies, Edge Act corporations, Agreement corporations, other U.S. insured depository institutions, foreign entities engaged in the business of banking which are regulated or supervised by a foreign bank regulatory or supervisory authority, and branches or affiliates of any of the foregoing regulated or supervised by a U.S. or foreign bank regulatory or supervisory authority or engaged solely in providing data processing services to a bank or financial institution. The definition of the term "financial institution" for these purposes includes U.S. entities engaged primarily in the business of issuing a general purpose charge, debit or stored value card. It is imperative that these definitions, which define the scope of Section 772, are not narrowed in any way that would preclude Visa or any of its member financial institutions from taking advantage of the provisions of Section 772 in connection with the Visa payments system.

Visa does, however, have one concern with the Interim Rule. Certain provisions of Section 772 are not available for certain Visa members located in certain

specified countries. While Visa understands the rationale for excluding certain countries from Section 772, these exclusions do create potential problems for worldwide payments systems like Visa's. As discussed above, the efficiencies and other benefits of the Visa payments system for Visa financial institution members and their customers depend upon the uniform operation of the system throughout the world. One of the core strengths of the Visa system is that any Visa cardholder can use his or her Visa card at any of the over 14 million locations around the world at which Visa is accepted. To the extent that aspects of the Visa system cannot be offered in a particular country as a result of a Section 772 exclusion, the benefits of the system for Visa cardholders desiring to engage in Visa transactions in that excluded country and for Visa financial institution members in that country are accordingly diminished. Visa urges the Commerce Department to consider limiting the countries excluded from Section 772 to as narrow a list as possible with respect to the export and reexport of non-recoverable payment-specific encryption software and commodities of any key length that are restricted by design (e.g., highly field-formatted with validation procedures, and not easily diverted to other uses) for payment system applications.

* * * * *

Visa very much appreciates this opportunity to comment on the Interim Rule. If you have any questions concerning this letter, please do not hesitate to contact me, at (650) 432-3161.

Sincerely,

Broox Peterson
Senior Vice President

exportad.doc

Legal Affairs Office
Citibank, N.A.
909 Third Avenue
32nd Floor
New York, NY
10043
212/559-0142
Fax
212/793-2516

P. Michael Nugent
General Counsel for
Technology and
Intellectual Property

#6 pg 1 of 7

CITIBANK

By Facsimile

November 6, 1998

Ms. Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
P.O. Box 273
Washington, D.C. 20044

Re: Citicorp Comments on September 22, 1998 Interim Rule on Financial and Other Encryption Export Controls

Dear Ms. Crowe:

On behalf of Citicorp, we hereby submit comments on the interim final rule published in 63 Fed. Reg. 50516 (Sept. 22, 1998) (hereinafter the "Rule"). The Rule adopted changes to the initial rule on Encryption Items published December 30, 1996 and implemented the Administration's liberalized policy for exports of general purpose encryption products to financial institutions and of financial specific products, a policy first announced in May 1997 and announced in revised form July 7, 1996. As you may recall, Citicorp submitted detailed comments to your department last summer on a draft version of this regulation dated July 25, 1997. We very much appreciate the extent to which you improved the final version of the regulations based in part on our earlier comments. This rule is indeed a vast improvement on the earlier draft, which demonstrates the sensibility of BXA soliciting comments on the rule in draft form. More work still needs to be done, and we hope that the following additional suggestions will help you to make this Rule even more workable for exporters. (Please note that we are commenting on how to improve the Rule within the context of the Administration's existing policy, but this focus in these comments should not be viewed as an endorsement of said policy.)

These comments are provided in the order of the regulations for your convenience.

#6 pg 2 of 7

EAR 734.2(b)(9)(ii)(A)

We appreciate your clarifications to EAR Sec. 734.2(b)(9)(ii)(A) and in particular your continued use of regulations to authorize in a reasonably practical way the practice of making encryption software available for electronic download as long as the person verifies based on information available (addresses) that the recipient is in the United States or Canada. This is a major improvement over the original proposed rule of July 1997.

EAR 734.2(b)(9)(ii)(C)

As written, the final sentence in this paragraph seems to suggest that BXA intends to review acknowledgments in electronic form before exporters may be permitted to use them, although we do not understand that this is what is intended. BXA has not previously imposed such a requirement, and Section 740.6(a)(e), as revised, permits assurances via facsimile, which is but one form of electronic acknowledgment. The Administration has long recognized the validity of clicking on an "I accept button" for example. The final sentence of Section 734.2(b)(9)(ii)(C) should be revised as follows: "Acknowledgments in electronic form are permitted provided that they are adequate to assure legal undertakings similar to written acknowledgments." This statement more clearly expresses what we understand is the intent of this provision.

EAR 740.6(a)(3)

We also suggest that you revise this section to clarify that all forms of electronic assurances are permitted, which we understand to be the current interpretation: "The required assurance may be made in the form of a letter or any other written communication from the importer, including electronic forms such as facsimile, e-mail or clicking on an "I accept button". The assurances may also be incorporated into a licensing agreement, a service agreement, or other contract."

EAR 740.8

It is confusing to exporters and to their customers to include non-recoverable items under License Exception KMI, which has until now been used solely for recoverable items. Customers think that exports under this provision embody a key recovery scheme, a perception that inhibits marketability of non-recoverable U.S. products. This confusion will be increased as the categories of acceptable non-recovery items expands. We therefore strongly recommend that you move the non-recovery items (Sec. 740.8(b)(2)(i), (ii), and (iii)) to a new license exception, such as License Exception

#6 pg 3 of 7

ENC which has been proposed following the September 16, 1998 announcement by Vice President Gore of further changes to encryption policy. The redundant portions of this paragraph (*e.g.*, subparagraphs (ii)(A)(2) and (iii)(A)(2)) could be stated at the beginning of the new License Exception entry.

EAR 740.8(b)(2)(ii) and the Long-Standing "Money and Banking" Exception

Exporters have long been permitted to self-classify commodities and software which are designed and limited for use in banking or money transactions (5A002/Related Controls (h) and by reference 5D002, which also existed as exceptions to encryption controls under the International Traffic in Arms Regulations). It is unclear at best what the difference is between items falling under these long-standing "money and banking" exceptions described in 5A002/5D002 and those falling under this new Section 740.8(b)(2)(ii) for financial specific encryption products. Financial-specific encryption items should continue to be reviewed via Advisory Opinions as an option, not on a mandatory basis. The new License Exception KMI provision calls for mandatory one-time review of the types of products that have for years been interpreted by the Department of State and the National Security Agency as falling under the provisions of the "money and banking exception." In order to be clear and consistent, and to avoid unnecessary requests for classifications, BXA should move all non-recoverable, financial specific items to ECCN 5A992/5D992 categories. This could be done via a new definition or a new interpretation. A new definition for "financial-specific" could include detailed language describing the criteria for eligibility (e.g., "highly field formatted with validation procedures and not easily diverted to other end-uses," "to secure financial communications/transactions for end-uses such as financial transfers or electronic commerce"), or the classification could be clarified in a new interpretation. It would be important to make clear in the definition that the concept of "securing financial communications/transactions" includes all forms of communication, such as e-mail.

EAR 740.8(b)(ii)(B and C)

We simply want to thank you for grandfathering prior products that have been reviewed for future exports under License Exception KMI to banks and financial institutions and under Encryption Licensing Arrangements. Such provisions to minimize needless applications are appreciated. We propose below that you expand this concept to clarify that future modifications that do not change the encryption functions materially do not require subsequent review, which we understand to be BXA's current interpretation but which is only now provided clearly for mass market software.

#6 pg 4&7

EAR 740.9 (a)(2)(ix)

We understand that this part was included because a similar provision was included in the ITAR. Because, under ITAR, software was considered part of hardware, we believe that software should be included here as well. The addition of software would also harmonize this subparagraph (ix) with Tools of the Trade (subparagraph (i)).

EAR 740 - Supplement No. 3

The limited list of countries whose banks and financial institutions are authorized to receive exports is an unwarranted roll back of authority that has been granted in the past for exports to banks and financial institutions in previously issued ELAs by the State as well as the Commerce Department. This puts exporters without existing ELAs at a disadvantage vis-à-vis those with ELAs, and subjects new products to tighter restrictions than older products even if the encryption used in the product is the same. We understand that this policy decision was a result of a compromise among different agencies. Nevertheless, this rollback undercuts the credibility of the Administration's already fragile encryption policy.

At minimum, the exporting community deserves to be told in advance which countries will be excluded from Encryption Licensing Arrangements to banks and financial institutions in destinations outside said 44 countries (except the seven embargoed and terrorist supporting countries). It is inappropriate not to list countries to which the U.S. will not allow such exports due to money laundering concerns. It appears that the Administration has put diplomatic concerns of not offending countries that do not adequately restrict money laundering ahead of the needs of exporters. Even with advance notification, this rollback of authorization to export products to banks in closely allied countries such as Mexico and other Latin American and Caribbean countries is unwarranted.

In addition, while we understand it was the intention to put branches of U.S. banks outside the U.S. on the same footing with branches of foreign banks, the fact that the U.S. is not included in this Supplement 3 list has led some of us to question whether we can rely solely on the definition of "Bank" to achieve that result. We appreciate Jim Lewis' verbal advice to those who ask that exporters may ship general purpose encryption items to branches of U.S. banks anywhere as was expressed in Commerce Secretary Daley's press release of July 7, 1998, but this is such a fundamental omission that BXA should put this advice in writing on its web guidance as well as correcting the rule to put such exports on a more sound legal basis. Including the "United States" on the list would provide exporters greater certainty on this issue.

#6 pg 5 of 7

EAR 742.15(b)(1) - Broaden Approval of Updating with Same Encryption

We very much appreciate the following clarification:

> Furthermore, for such software released from EI controls, subsequent bundling, updates, or releases consisting of or incorporating this software may be exported and reexported without a separate one-time technical review, so long as the functional encryption capacity (e.g., algorithm, key modulus) of the originally reviewed mass-market encryption software has not been modified or enhanced.

This concept has been applied to other provisions and should not be limited to the mass marketing context. We recommend that you add it to the provisions for general purpose encryption products for banks and financial institutions, the financial specific provisions, and to others being developed. It would be better to place this provision in a more generally applicable interpretation section at the beginning or the end of EAR Part 742.14 and/or 740.8 so that exporters will clearly know that subsequent versions of products are still covered by a one time review unless the encryption functions have changed materially. This has long been BXA's interpretation.

EAR 742 - Supplement 4

We recommend that BXA add the following phrase after the word "inoperative" at the end of Paragraph (6)(i) of this Supplement: " . . .unless the operable key recovery product produces the key recovery information for all transactions between it and the product with inoperative key recovery features."

EAR Part 772 – Definition of "Bank"

As drafted in the interim regulations, Subparagraph (e) of this definition appears to cover only those "affiliates" whose sole and exclusive business is providing data processing services to banks or financial institutions. In our experience, many entities that provide data processing services to banks and financial institutions also provide similar services to non-financial organizations. In addition, these "affiliates" may also develop data processing services and products. Therefore, we suggest that the paragraph be revised to read: "An affiliate of any of the entities listed in paragraphs (a), (b), (c) or (d) of this definition, when it is engaged by the entity for the purpose of developing or

#6 pg 6 of 7

providing data processing services or products to a bank or financial institution, or a branch of such an affiliate."

EAR Part 772 – Definition of "Effective control"

We are concerned that identifying specific security measures, such as hotel safes, makes the definition more confusing and unnecessarily restrictive. For example, to protect sensitive business information, many business travelers take precautions to protect the software and data on laptops, such as password protecting "boot up" or encrypting the contents of the hard drive. Requiring the use of a safe or bonded warehouse is inconsistent with modern business practices and would effectively gut the laptop exemption for some business travelers. We believe that the intent of "effective control" is to require the exporter to take positive steps to protect the items being temporarily exported or re-exported. Trying to define the many ways in which an item might be secured is probably unrealistic.

Therefore, we suggest that the definition be simplified as follows: "You maintain effective control over an item when you retain physical possession of the item or take other steps to secure the item." Alternatively, we suggest that BXA consider not defining the term at all.

EAR Part 772 – Definition of "Financial Institution"

Comment 1: The definition should include clearing or settlement services as mentioned in subparagraph (c)of the definition of "Bank."

Comment 2: We suggest that subparagraph (f) be revised in a manner similar to the suggested revision for subparagraph (c) in the definition of "Bank."

EAR Part 774 – CCL Categories 5A002 and 5D002

It would be extremely helpful to create different classification categories for items removed from EI controls. It is very confusing for many exporters whose systems are geared to control items by their ECCNs to discriminate between ECCN 5D002.c.1 EI controlled items that require a license to every destination and 5D002.c.1 non-EI controlled items that are eligible for export to all but seven countries under License Exception TSU. The "classification" appears meaningless. We assume that Customs has similar problems.

#6 pg 7 of 7

The following statement should be eliminated from the first note to ECCN 5D002: "License Exceptions for commodities are not applicable." This is confusing and not necessary, as many license exceptions that are generally used primarily for commodities have been considered by BXA to be applicable to encryption software (TMP, BAG, GOV, etc.).

We appreciate the opportunity to comment of these regulations. Please do not hesitate to contact either of the undersigned or Ben Flowe of Berliner, Corcoran & Rowe, L.L.P. (202-293-6117) if you have questions or wish to discuss any of these comments.

Respectfully submitted,

Michael Nugent
General Counsel for Technology and
Intellectual Property

Steve Katz
Vice President & Chief
Information Security Officer

cc: Mr. James Lewis
Ms. Patricia Sefcik

=7 pg 183

STEPTOE & JOHNSON LLP

1330 Connecticut Avenue, NW
Washington, DC 20036-1795

Telephone 202.429.3000
Facsimile 202.429.3902
http://www.steptoe.com

R. N. "Fritz" Fielding
202.429.6468
rfieldin@steptoe.com

November 6, 1998

Ms. Nancy Crowe
Regulatory Policy Division
P.O. Box 273
Department of Commerce
Washington, D.C. 20044

Re: Interim Rule Promulgated on September 22, 1998 (63 Fed. Reg. 50516)

Dear Ms. Crowe:

The Interim Rule published in September 1998, 63 Fed. Reg. 50516, clarified many of the provisions of the EAR that relate to encryption items. The Interim Rule, however, did not address technical assistance. Since the Department of Commerce assumed responsibility for commercial encryption exports, it has become apparent that the scope of the technical assistance provision (15 C.F.R. § 744.9) needs clarification. We urge you to provide such clarity as soon as possible.

As you know, the technical assistance provision is unique to the encryption control regime. It requires an export license if a U.S. person is providing technical assistance to a foreign national with the intent of aiding in the development or manufacture of encryption commodities or software that would be controlled for EI reasons by the U.S. The difficulty with this language is that a literal reading, uninformed by policy, could lead to the mistaken impression that the provision covers any assistance regardless of whether the assistance relates to encryption. Since we doubt that the Commerce Department intends such results, we recommend revising the language to bring into accord with policy.

By way of illustration, consider the situation in which a U.S. engineer is asked to assist a foreign person to debug a radio or software program that includes Triple DES, general-purpose data encryption. Let's assume that the assistance does not relate to the encryption features of the radio or software. Would the U.S. require an export license before the engineer provided such assistance? As noted above, a literal reading of the language of the technical assistance provision

would suggest a "yes" answer. The U.S. engineer is providing what would appear in lay terms to be technical assistance. The assistance is provided to a foreign person. The assistance is provided with the intent of aiding the foreign person in the manufacture of a radio or software program that includes encryption the U.S. would control for EI reasons.

Consider another scenario. A U.S. company produces widgets with encryption. The widget with the encryption is controlled for EI reasons. (Without the encryption it would not be controlled.) Because the U.S. company wants the world to standardize on its technology, it develops a protocol document that it proposes to distribute to interested parties around the world. The protocol provides a technical description of how the various features of the widget operate, including the encryption feature. In the encryption portion of the protocol, the U.S. company merely identifies the encryption algorithm as well as how the encryption is keyed and a high level description of how the encryption will interface with the rest of the widget. However, it does not provide the encryption or key management algorithms, much less the cryptographic API or other code that would make the encryption functional.

The protocol documents are technology, but not likely controlled technology as they do not include the encryption or the details of the interface. But does provision of the protocol constitute controlled technical assistance? Again, a literal reading of the regulations would seem to suggest a "yes" answer. The protocols are technical data and providing them would certainly assist the recipient. Moreover, by the terms of this scenario, the protocols are provided to a foreign person with the intent that such person can produce the widget with encryption, albeit once they obtain the raw materials and the encryption.

Whether intended or not, it is easy to see how such a literal reading of this provision could have a chilling effect on legitimate commercial activities. Companies either forego the opportunity to provide assistance or they incur the costs and delays inherent in obtaining a license (or an opinion that a license is not required). This chilling effect is particularly troubling where, as in the second scenario, the assistance takes the form of the provision of technology. Arguably, technology is speech protected by the First Amendment.

The Government is addressing the First Amendment implications of technology controls in the context of ongoing litigation challenging its regulation of encryption software and source code exports. The Government's position in that litigation is that the controls are proper because, in contrast to other types of software, encryption software/source code provides the very functionality that gives rise to the national security interest in encryption. Even if encryption software or source code is considered protected speech, the Government's controls have only an incidental impact on that speech and are no more restrictive than necessary to achieve legitimate national security interests.

The Constitutional merits of the Government's arguments remain to be seen. However, the Government is to be commended for staking out a position that tries to limit the impact of the regulations by focusing on the principle interest at stake, i.e., controlling the export of functional encryption capabilities. Unfortunately, the broad impact that a literal reading of the technical assistance provision permits is inconsistent with the position the Government has taken in the litigation and serves to aggravate the chilling effect noted above. Therefore, we urge the Commerce Department to take quick action to clarify that the scope of the technical assistance provision is not intended to restrict activities other than those required to achieve encryption functionality. We specifically recommend using the term "required" in the clarification. It is a defined term in the Export Administration Regulations (EAR) that exporters have worked with over the years. This history will aid exporters in understanding when technical encryption assistance requires an export license.

If you have any question, please call me.

Sincerely,

R.N. Fielding

RNF:jb